Quest® One

ActiveRoles® 6.8

Administratorhandbuch

QUEST SOFTWARE®
Simplicity At Work®

© 2013 Quest Software, Inc.
ALLE RECHTE VORBEHALTEN.

Dieses Handbuch enthält urheberrechtlich geschützte Informationen. Die im vorliegenden Handbuch beschriebene Software unterliegt den Bedingungen der jeweiligen Softwarelizenz oder Geheimhaltungsvereinbarung. Die Software darf nur gemäß den Bestimmungen der gültigen Vereinbarung verwendet oder kopiert werden. Die Vervielfältigung und die Übermittlung des vorliegenden Handbuchs oder seiner Teile in anderen elektronischen oder gedruckten Publikationen ist ohne ausdrückliche Zustimmung von Quest Software, Inc., nicht gestattet. Dies gilt nicht, wenn die Informationen zum ausschließlichen privaten Gebrauch eines Nutzers bestimmt sind.

Die Informationen in diesem Dokument werden in Verbindung mit Quest-Produkten zur Verfügung gestellt. Durch dieses Dokument wird weder explizit noch implizit, durch Duldungsvollmacht oder auf andere Weise, eine Lizenz auf intellektuelle Eigentumsrechte erteilt, auch nicht in Verbindung mit dem Erwerb von Quest-Produkten. MIT AUSNAHME DER BESTIMMUNGEN IN DEN ALLGEMEINEN GESCHÄFTSBEDINGUNGEN VON QUEST, DIE IN DER LIZENZVEREINBARUNG FÜR DIESES PRODUKT AUFGEFÜHRT SIND, ÜBERNIMMT QUEST KEINERLEI HAFTUNG UND SCHLIESST JEDE EXPLIZITE, IMPLIZITE ODER GESETZLICHE GEWÄHRLEISTUNG FÜR SEINE PRODUKTE AUS, INSBESONDERE DIE IMPLIZITE GEWÄHRLEISTUNG DER MARKTFÄHIGKEIT, DER EIGNUNG ZU EINEM BESTIMMTEN ZWECK UND DIE GEWÄHRLEISTUNG DER NICHTVERLETZUNG VON RECHTEN. UNTER KEINEN UMSTÄNDEN HAFTET QUEST FÜR UNMITTELBARE, MITTELBARE ODER FOLGESCHÄDEN, SCHADENERSATZ, BESONDERE ODER KONKRETE SCHÄDEN (INSBESONDERE SCHÄDEN, DIE AUS ENTGANGENEN GEWINNEN, GESCHÄFTSUNTERBRECHUNGEN ODER DATENVERLUSTEN ENTSTEHEN), DIE SICH DURCH DIE NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DIESES DOKUMENTS ERGEBEN, AUCH WENN QUEST ÜBER DIE MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE. Quest übernimmt keine Garantie für die Richtigkeit oder Vollständigkeit der Inhalte dieses Dokuments und behält sich vor, jederzeit und ohne vorherige Ankündigung Änderungen an den Spezifikationen und Produktbeschreibungen vorzunehmen. Quest geht keinerlei Verpflichtung ein, die in diesem Dokument enthaltenen Informationen zu aktualisieren.

Bei Fragen zur möglichen Verwendung dieser Materialien wenden Sie sich bitte an:

Quest Software World Headquarters
LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656
E-Mail: legal@quest.com

Informationen über unsere lokalen und internationalen Büros finden Sie auf unserer Website (www.quest.com).

Warenzeichen

Quest, Quest Software, das Quest Software-Logo, Simplicity at Work und ActiveRoles sind Warenzeichen oder eingetragene Warenzeichen von Quest Software, Inc. Eine vollständige Liste der Warenzeichen von Quest Software finden Sie unter http://www.quest.com/legal/trademarks.aspx. Andere Warenzeichen sind Eigentum ihrer jeweiligen Besitzer.

Beiträge von Drittanbietern

Dieses Produkt enthält einige Komponenten von Drittanbietern (nachfolgend aufgelistet). Kopien der Lizenzen dieser Drittanbieter finden Sie unter http://www.quest.com/legal/third-party-licenses.aspx. Der Quellcode für die mit einem Sternchen (*) markierten Komponenten ist verfügbar unter http://rc.quest.com.

KOMPONENTE	LIZENZ ODER BESTÄTIGUNG
.NET logging library 1.0	BSD 4.4-Lizenz
JQuery 1.7.1	MIT 1.0-Lizenz
JQuery UI 1.8.14	MIT 1.0-Lizenz
ObjectBuilder 2.2.0.0	Enthält Software oder andere Inhalte, die auf Basis von Schemata und Praktiken von Microsoft adaptiert wurdenObjectBuilder, © 2006 Microsoft Corporation. Alle Rechte vorbehalten.

Quest One ActiveRoles - Administratorhandbuch
Aktualisiert - März 01, 2013
Softwareversion - 6.8

INHALT

ÜBER DIESES HANDBUCH 11

ZIELGRUPPE DIESES HANDBUCHS 12

FORMATIERUNGSKONVENTIONEN 12

ÜBER QUEST SOFTWARE, INC. 13

KONTAKT ZU QUEST SOFTWARE 13

KONTAKT ZUM QUEST SUPPORT 13

EINLEITUNG 14

KAPITEL 1
ÜBER QUEST ONE ACTIVEROLES 15

WAS IST QUEST ONE ACTIVEROLES? 16

DAS BIETET QUEST ONE ACTIVEROLES 17

WARUM QUEST ONE ACTIVEROLES? 20

TECHNISCHE ÜBERSICHT. 22

PRÄSENTATIONSKOMPONENTEN 23

DIENSTKOMPONENTEN 24

NETZWERKDATENQUELLEN 25

SICHERHEITS- UND VERWALTUNGSELEMENTE 26

SICHERHEITSVERWALTUNG FÜR ACTIVE DIRECTORY. 29

ADSI-PROVIDER UND SKRIPTRICHTLINIE ZUR UNTERSTÜTZUNG DER ANPASSUNG 30

DYNAMISCHE GRUPPEN 31

BETRIEB IN UMGEBUNGEN MIT MEHREREN GESAMTSTRUKTUREN 32

KAPITEL 2
ERSTE SCHRITTE 35

STARTEN DER QUEST ONE ACTIVEROLES-KONSOLE 36

ERHALTEN UND VERWENDEN DER HILFE 36

ÜBERBLICK ÜBER DIE BENUTZERSCHNITTSTELLE 37

ANZEIGEMODUS 39

VERWENDEN VERWALTETER EINHEITEN 40

EINRICHTEN EINES FILTERS 41

SUCHEN NACH OBJEKTEN 42

ABRUFEN RICHTLINIENBEZOGENER INFORMATIONEN. 47

KAPITEL 3
REGELBASIERTE ADMINISTRATIVE ANSICHTEN 49

VERWALTETE EINHEITEN 50

FUNKTIONSWEISE VERWALTETER EINHEITEN 50

ADMINISTRATION VERWALTETER EINHEITEN 51

ERSTELLEN EINER VERWALTETEN EINHEIT. 51

Anzeigen der Mitglieder einer verwalteten Einheit 61
Hinzufügen und Entfernen von Mitgliedern einer verwalteten Einheit 63
Kopieren einer verwalteten Einheit 67
Exportieren und Importieren einer verwalteten Einheit 68
Umbenennen einer verwalteten Einheit 69
Löschen einer verwalteten Einheit 69
Szenario: Implementieren der rollenbasierten Verwaltung über mehrere Organisationseinheiten hinweg 70
Überlegungen bezüglich der Bereitstellung 71
Mitgliedschaftsregeln für die verwaltete Einheit 72
Delegieren von verwalteten Einheiten 73

Kapitel 4
Rollenbasierte Administration 75
Zugriffsvorlagen zum Definieren von Administratorfunktionen 76
Funktionsweise von Zugriffsvorlagen 76
Sicherheitssynchronisierung 77
Verwaltungsaufgaben für Zugriffsvorlagen 78
Verwenden vordefinierter Zugriffsvorlagen 78
Erstellen einer Zugriffsvorlage 81
Anwenden von Zugriffsvorlagen 91
Verwalten von Zugriffsvorlagenverknüpfungen 97
Synchronisieren von Berechtigungen mit Active Directory 102
Hinzufügen, Ändern und Entfernen von Berechtigungen 105
Schachteln von Zugriffsvorlagen 108
Kopieren einer Zugriffsvorlage 110
Exportieren und Importieren von Zugriffsvorlagen 111
Umbenennen einer Zugriffsvorlage 112
Löschen einer Zugriffsvorlage 112
Verwendungsbeispiele 113
Szenario 1: Implementieren eines Help Desk 113
Szenario 2: Implementieren der Selbstverwaltung 115
Überlegungen bezüglich der Bereitstellung 118
Delegation der Administration einer Organisationseinheit 119
Delegieren der Gruppenadministration 120
Delegation in einer funktionalen Umgebung im Vergleich zu einer gehosteten Umgebung 121

Kapitel 5
Regelbasierte automatische Bereitstellung und Deprovisionierung 123
Richtlinienobjekte 124
Bereitstellungsrichtlinienobjekte 125

Deprovisionsrichtlinienobjekte 127
Funktionsweise von Richtlinienobjekten 128
Verwaltungsaufgaben für Richtlinienobjekte 130
Erstellen eines Richtlinienobjekts 130
Hinzufügen, Ändern und Entfernen von Richtlinien 133
Anwenden von Richtlinienobjekten 136
Verwalten des Richtlinienbereichs 140
Kopieren eines Richtlinienobjekts 147
Umbenennen eines Richtlinienobjekts 147
Exportieren und Importieren von Richtlinienobjekten 148
Löschen eines Richtlinienobjekts 149
Konfigurationsaufgaben für Richtlinien 150
Erzeugung und Validierung von Eigenschaften 150
Erzeugung von Benutzeranmeldenamen 171
Automatische Bereitstellung der Gruppenmitgliedschaft 182
E-Mail-Aliaserzeugung 189
Automatische Bereitstellung des Exchange-Postfachs 195
Stammordner AutoProvisioning 201
Skriptausführung 213
Benutzerkonto-Deprovisionierung 221
Entfernung der Gruppenmitgliedschaft 234
Exchange-Postfach-Deprovisionierung 240
Stammordner-Deprovisionierung 244
Benutzerkonto-Verschiebung 248
Permanentes Löschen des Benutzerkontos 251
Gruppenobjekt-Deprovisionierung 254
Gruppenobjekt-Verschiebung 263
Dauerhaftes Löschen des Gruppenobjekts 266
Benachrichtigungsverteilung 269
Berichtsverteilung 274
Überlegungen bezüglich der Bereitstellung 279
Überprüfen der Richtlinieneinhaltung 282
Deprovisionieren von Benutzern oder Gruppen 287
Standardoptionen für die Deprovisionierung 287
Delegieren der Deprovisionsaufgabe 288
Verwenden des Deprovisionsbefehls 289
Bericht zu Ergebnissen der Deprovisionierung 290
Wiederherstellen von deprovisionierten Benutzern oder Gruppen 297
Richtlinienoptionen für die Aufhebung der Deprovisionierung eines Benutzers 298

Delegieren der Aufhebung der Deprovisionierung 299
Verwenden des Befehls zur Aufhebung der Deprovisionierung 300
Bericht über die Ergebnisse der Aufhebung der Deprovisionierung 301
Richtlinie zur Vermeidung einer Containerlöschung 305
Objekte vor versehentlichem Löschen schützen 306
Richtlinienerweiterungen 309
Designelemente 309
Erstellen und Verwalten von benutzerdefinierten Richtlinientypen 311

Kapitel 6
Arbeitsabläufe 319
Beschreibung des Arbeitsablaufs 320
Wichtige Funktionsmerkmale und Definitionen 320
Arbeitsablaufprozesse 322
Übersicht über die Arbeitsablaufverarbeitung 323
Übersicht über die Arbeitsablaufaktivitäten 326
Genehmigungsaktivität 326
Benachrichtigungsaktivität 331
Skriptaktivität 332
Wenn-Dann-Genehmigungsaktivität 333
Aktivität stoppen/unterbrechen 337
Aktivität „Berichtsabschnitt hinzufügen“ 337
Suchaktivität 338
CRUD-Aktivitäten 350
Konfigurieren eines Arbeitsablaufs 362
Erstellen einer Arbeitsablaufdefinition 362
Konfiguration der Workflow-Start-Bedingungen 363
Workflow-Parameter konfigurieren 371
Hinzufügen von Aktivitäten zu einem Arbeitsablauf 374
Konfigurieren einer Genehmigungsaktivität 374
Konfigurieren einer Benachrichtigungsaktivität 382
Konfigurieren einer Skriptaktivität 385
Konfigurieren einer Wenn-Dann-Sonst-Aktivität 386
Konfigurieren einer Stoppen/Unterbrechen-Aktivität 391
Konfiguration einer Aktivität „Berichtsabschnitt hinzufügen“ 391
Konfigurieren einer Suchaktivität 393
Konfiguration von CRUD-Aktivitäten 404
Aktivieren oder Deaktivieren einer Aktivität 420
Aktivieren oder Deaktivieren eines Arbeitsablaufs 420

Beispiel: Genehmigungs-Arbeitsablauf 421
Begriffsdefinition 422
Funktionsweise 423
Erstellen und Konfigurieren eines Genehmigungs-Arbeitsablaufs . . 427
E-Mail-basierte Genehmigung 431
Integration in Microsoft Outlook 431
Integration in andere E-Mail-Clients als Outlook 432
E-Mail-Übertragung über Exchange Web Services 433
Automatisierungs-Arbeitsablauf 436
Optionen und Startbedingungen des Arbeitsablaufs „Automatisierung" 436
Verwenden des Automatisierungs-Arbeitsablaufs 440
Aktivitätserweiterungen 450
Designelemente 450
Erstellen und Verwalten von benutzerdefinierten Aktivitätstypen 452

Kapitel 7
Temporare Gruppenmitgliedschaften 459
Beschreibung von temporären Gruppenmitgliedschaften 460
Verwenden von temporären Gruppenmitgliedschaften 463
Hinzufügen von temporären Mitgliedern 463
Anzeigen von temporären Mitgliedern 464
Neuplanen von temporären Gruppenmitgliedschaften 465
Entfernen von temporären Mitgliedern 466

Kapitel 8
Gruppenfamilie 467
Grundlegendes zu Gruppenfamilien 468
Entwurfsübersicht 468
Funktionsweise 469
Erstellen einer Gruppenfamilie 471
Starten des Assistent für neue Gruppenfamilie 471
Name der Gruppenfamilie 472
Gruppierungsoptionen 473
Ort der verwalteten Objekte 474
Auswahl der verwalteten Objekte 475
Gruppieren-nach-Eigenschaften 477
Vorhandene Gruppen manuell erfassen 478
Gruppenbenennungsregel 479
Gruppenbereich und -typ 482
Ort der Gruppen 483

Exchange-bezogene Einstellungen 484
Planung für Gruppenfamilie 485
Zusammenfassung: Verfahren zur Erstellung einer Gruppenfamilie 486
Verwalten einer Gruppenfamilie 489
Kontrollierte Gruppen 490
Registerkarte „Allgemein" 491
Registerkarte „Kontrollierte Gruppen" 492
Registerkarte „Gruppierungen" 495
Registerkarte „Zeitplan" 496
Registerkarte „Vorgangsübersicht" 496
Zusammenfassung: Verfahren zur Verwaltung einer Gruppenfamilie 498
Szenario: Abteilungsbezogene Gruppenfamilie 499

Kapitel 9
Dynamische Gruppen 501
Grundlegendes zu dynamischen Gruppen 502
Richtlinie zu dynamischen Gruppen 503
Verwalten dynamischer Gruppen 504
Konvertieren einer Standardgruppe in eine dynamische Gruppe 504
Anzeigen der Mitglieder einer dynamischen Gruppe 506
Hinzufügen einer Mitgliedschaftsregel zu einer dynamischen Gruppe 506
Entfernen einer Mitgliedschaftsregel aus einer dynamischen Gruppe 508
Konvertieren einer dynamischen Gruppe in eine Standardgruppe 509
Ändern, Umbenennen oder Löschen einer dynamischen Gruppe 509
Szenario: Automatisches Verschieben von Benutzern zwischen Gruppen 509

Kapitel 10
Berichte in Quest One ActiveRoles 513
Einleitung 514
Datenvorbereitungs-Collector für Berichte 515
Sammeln von Daten aus dem Netzwerk 516
Verarbeiten gesammelter Ereignisse 520
Quest Knowledge Portal für die Anzeige von Berichten 521
Arbeiten mit Berichten 523

Kapitel 11
Verwaltungsverlauf 533
Beschreibung des Verwaltungsverlaufs 534
Überlegungen und optimale Vorgehensweisen 534

Konfiguration des Verwaltungsverlaufs 537
Richtlinie für die Änderungsnachverfolgung 537
Konfiguration des Verfolgungsprotokolls ändern 538
Replikation von Verwaltungsverlaufsdaten 539
Zentralisierte Verwaltungsverlaufsspeicherung 541
Untersuchen des Änderungsverlaufs 546
Arbeitsablaufaktivität – Berichtsabschnitte 548
Berichtselemente der Richtlinie 553
Berichtselemente der internen Richtlinie von ActiveRoles 556
Untersuchen von Benutzeraktivitäten 563

Kapitel 12
Berechtigungsprofil 565
Verstehen des Berechtigungsprofils 566
Informationen zu Berechtigungsprofilspezifizierern 567
Konfiguration des Berechtigungsprofils 571
Erstellen von Berechtigungsprofil-Spezifizierern 571
Ändern von Berechtigungsprofil-Spezifizierern 574
Vordefinierte Spezifizierer 576
Anzeigen des Berechtigungsprofils 580

Kapitel 13
Papierkorb 583
Beschreibung der Papierkorbfunktion 584
Suchen und Auflisten gelöschter Objekte 584
Wiederherstellen eines gelöschten Objekts 586
Delegieren von Vorgängen an gelöschten Objekten 587
Anwenden von Richtlinien- oder Arbeitsablaufregeln 588

Kapitel 14
AD LDS-Datenverwaltung 591
Registrieren einer AD LDS-Instanz 592
Verwalten von AD LDS-Objekten 593
Hinzufügen eines AD LDS-Benutzers zum Verzeichnis 594
Hinzufügen einer AD LDS-Gruppe zum Verzeichnis 595
Hinzufügen oder Entfernen von Mitgliedern zu bzw. aus einer AD LDS-Gruppe 595
Deaktivieren oder Aktivieren eines ADLDS-Benutzerkontos 596
Festlegen oder Ändern des Kennworts eines ADLDS-Benutzers 596
Hinzufügen einer Organisationseinheit zum Verzeichnis 597
Hinzufügen eines AD LDS (ADAM)-Proxyobjekts (Benutzerproxy) . . 597
Konfigurieren von Quest One ActiveRoles für AD LDS 598
In diesem Abschnitt wird jede dieser Aufgaben eingehend beschrieben 599

Anzeigen oder Festlegen von Berechtigungen für ADLDS-Objekte . . 600
Anzeigen oder Festlegen von Richtlinien für ADLDS-Objekte 601

Kapitel 15
Verwaltung der Einrichtungseinstellungen von Quest One ActiveRoles . 603

Einleitung 604
Herstellen einer Verbindung zum Verwaltungsdienst 604
Hinzufügen und Entfernen verwalteter Domänen 606
Konfigurieren von nicht verwalteten Domänen 608
Lizenzieren von nicht verwalteten Domänen 610
Registrieren einer nicht verwalteten Domäne 611
Konfigurieren der Replikation 612
Grundlegendes zum Replikationsmodell 612
Konfigurieren von SQL Server 613
Erstellen einer Replikationsgruppe 614
Hinzufügen von Mitgliedern zu einer Replikationsgruppe 614
Entfernen von Mitgliedern aus einer Replikationsgruppe 617
Überwachung der Replikation 618
Verwenden der Datenbankspiegelung 619
Einrichtung der Datenbankspiegelung in Quest One ActiveRoles . . . 620
Erstellen und Verwenden virtueller Attribute 621
Szenario: Implementieren eines Attributs für den Geburtstag 622
Untersuchen von Client-Sitzungen 624
Überwachen der Leistung 625
Anpassen der Konsole 626
Seite „Andere Eigenschaften" im Objekterstellungsassistent 626
Registerkarte „Andere Eigenschaften" im Dialogfeld „Eigenschaften" 628
Anpassen von Anzeigenamen 629
Änderung des Administratorenkontos für ActiveRoles 630
Das Programm zur Verbesserung der Software 631

Kapitel 16
Anhang 633

Anhang A: Verwenden regulärer Ausdrücke 634
Rangfolge 636
Anhang B: Administrative Vorlage für ActiveRoles 637
Quest One ActiveRoles Snap-in-Einstellungen 637
Verwaltungsdiensteinstellungen für automatische Verbindung 639
Installationsanweisungen 641
Anhang C: Ports für Datenübertragung 642

Über dieses Handbuch

- Zielgruppe dieses Handbuchs
- Formatierungskonventionen
- Über Quest Software, Inc.
- Kontakt zu Quest Software
- Kontakt zum Quest Support
- Einleitung

Zielgruppe dieses Handbuchs

Dieses Dokument wurde erstellt, um Sie mit Quest® One ActiveRoles® vertraut zu machen. Das „Administratorhandbuch" enthält die erforderlichen Informationen zur Installation und Verwendung von Quest One ActiveRoles. Es wurde als Nachschlagewerk für Netzwerkadministratoren, Berater, Analysten und andere IT-Fachleute entwickelt.

Formatierungskonventionen

In diesem Handbuch werden bestimmte Formatierungskonventionen eingehalten, die die effektive Verwendung des Dokuments sicherstellen. Diese Konventionen werden auf unterschiedliche Vorgänge, Symbole, Tastenkombinationen und Querverweise angewandt.

ELEMENT	KONVENTION
Wählen	Dieses Wort bezieht sich auf Vorgänge wie das Auswählen oder Markieren diverser Benutzeroberflächenelemente wie zum Beispiel Dateien und Optionsfelder.
Fettdruck	In Quest Software-Produkten angezeigte Benutzeroberflächenelemente wie zum Beispiel Menüs und Befehle.
Kursivdruck	Wird für Anmerkungen verwendet.
Fetter Kursivdruck	Wird zur Hervorhebung verwendet.
Blaue Schrift	Zeigt einen Querverweis an. Kann in Adobe® Reader® als Hyperlink verwendet werden.
	Wird zum Hervorheben zusätzlicher Informationen verwendet, die für den jeweils beschriebenen Vorgang sachdienlich sind.
	Wird für empfohlene Vorgehensweisen verwendet. Eine empfohlene Vorgehensweise beschreibt einen Ablauf von Vorgängen detailliert, um optimale Ergebnisse zu erzielen.
	Damit werden Vorgänge hervorgehoben, die mit Vorsicht durchzuführen sind.
+	Ein Pluszeichen zwischen zwei Tasten bedeutet, dass beide Tasten gleichzeitig gedrückt werden müssen.
|	Ein senkrechter Strich zwischen Elementen bedeutet, dass Sie die Elemente in genau der angegebenen Reihenfolge auswählen müssen.

Über Quest Software, Inc.

Das im Jahr 1987 gegründete Unternehmen Quest Software (Nasdaq: QSFT) bietet einfache und innovative IT-Management-Lösungen, die es weltweit mehr als 100.000 Kunden ermöglichen, in physikalischen und virtuellen Umgebungen beträchtliche Zeit- und Kosteneinsparungen zu erzielen. Die Produkte von Quest lösen komplexe IT-Aufgaben von der Datenbankverwaltung, den Schutz der Daten über das Identitäts- und Zugangsmanagement und das Monitoring bis hin zum User Workspace Management oder das Windows Management. Weitere Informationen finden Sie unter www.quest.com.

Kontakt zu Quest Software

E-Mail	info@quest.com
Postanschrift	Quest Software, Inc. World Headquarters 5 Polaris Way Aliso Viejo, CA 92656 USA
Website	www.quest.com

Informationen über unsere lokalen und internationalen Büros finden Sie auf unserer Website.

Kontakt zum Quest Support

Der Support von Quest ist für Kunden verfügbar, die über eine Evaluierungsversion eines Quest-Produkts verfügen oder die ein Quest-Produkt erworben haben und über einen gültigen Wartungsvertrag verfügen. Der Quest-Support steht Ihnen rund um die Uhr an allen Wochentagen zur Verfügung unter unserem Serviceportal www.quest.com/support.

Auf unserem Support-Portal stehen Ihnen folgende Funktionen zur Verfügung:

- Abruf Tausender Lösungen aus unserer Knowledgebase
- Download der neuesten Versionen und Service Packs
- Erstellen, Aktualisieren und Überprüfen von Support-Fällen

Eine ausführlichere Erläuterung zu den Support-Programmen und zu den Online-Diensten sowie Kontaktinformationen und Angaben zu Richtlinien und Verfahren finden Sie im ***Global Support Guide***. Dieses Handbuch ist verfügbar unter: www.quest.com/support.

Einleitung

Das *Quest One ActiveRoles-Administratorhandbuch* richtet sich an Personen, die für die Implementierung der administrativen Struktur von Quest One ActiveRoles verantwortlich sind. Dieses Dokument bietet konzeptionelle Informationen zum Produkt und enthält systematische Vorgehensweisen für die Einrichtung einer sicheren, dezentralen Verwaltungsstruktur, die die Durchsetzung administrativer Richtlinien, die rollenbasierte Delegierung von Verwaltungsrechten und flexible administrative Ansichten kombiniert.

Das *Quest One ActiveRoles-Administratorhandbuch* wird durch das *Quest One ActiveRoles-Benutzerhandbuch* ergänzt, das Informationen über die Benutzeroberfläche der Quest One ActiveRoles-Konsole umfasst und die Verfahren erläutert, die delegierte Administratoren und Help Desk-Mitarbeiter bei der Durchführung der alltäglichen Verwaltungstätigkeiten mit Hilfe der Quest One ActiveRoles-Konsole unterstützen.

1

Über Quest One ActiveRoles

- Was ist Quest One ActiveRoles?
- Das bietet Quest One ActiveRoles
- Warum Quest One ActiveRoles?
- Technische Übersicht

Was ist Quest One ActiveRoles?

Mit der Entwicklung von Unternehmensnetzwerken hin zu verteilten, auf Client-Diensten basierenden Infrastrukturen steigt die Notwendigkeit einer inkrementellen Verwaltung. Dies veranlasst Organisationen zur Vereinfachung von Verwaltungsaufgaben, zur Steigerung der Sicherheit und zur Reduzierung der Netzwerkkosten. Quest One ActiveRoles erfüllt diese Ansprüche durch folgende Funktionen:

- Die Fähigkeit, Geschäftsregeln und administrative Richtlinien zur Sicherung des Sicherheitsmodells durchzusetzen, genügt allen organisatorischen Anforderungen.
- Die Fähigkeit, Kontrolle basierend auf anpassbaren Administratorfunktionen zu delegieren. Dies vereinfacht die Verwaltung von Active Directory vom Zeitpunkt der Einrichtung an.
- Die Fähigkeit, Berechtigungen in Quest One ActiveRoles festzulegen und zu ändern sowie diese Änderungen automatisch an Active Directory weiterzugeben.
- Die Fähigkeit, flexible, regelorientierte administrative Ansichten einzurichten, die die Verwaltung Active Directory-basierter Unternehmen über geografische Grenzen sowie über die Hierarchie von Organisationseinheiten hinweg ermöglichen.
- Die Fähigkeit, Verwaltungs- und Bereitstellungsaufgaben zu automatisieren, die einen vordefinierten, bedingungsgesteuerten Workflow aufweisen. So wird die Produktivität von Administratoren erhöht, und kostspielige Fehler werden vermieden.
- Sichere Verwaltung von Active Directory-Daten (Benutzerkonten, Gruppen, Computerkonten etc.) durch Richtlinieneinschränkungen und Automatisierungsfunktionen, die das Verbleiben veralteter Daten im Verzeichnis verhindern.
- Automatisierte, regelorientierte Verwaltung von Sicherheits- und Verteilergruppen. Diese ermöglicht die automatische Auffüllung von Gruppen und erhöht somit die Genauigkeit und Zuverlässigkeit.
- Verwaltung und Bereitstellung von Exchange-Postfächern.
- Überprüfung der Benutzerverwaltung und erweiterte Berichterstattung. Ein umfangreiches Paket von Berichten für die Verwaltung von Active Directory und Exchange kann zur Überprüfung anhand der Änderungsnachverfolgung, für die Durchsetzung von Unternehmensrichtlinien sowie die Überwachung und Analyse von Active Directory verwendet werden.
- Einfach zu verwendende Benutzeroberflächen, um die Netzwerkverwaltung zu optimieren und den Verwaltungsaufwand sowie die Kosten zu reduzieren.

Quest One ActiveRoles baut auf dem Verwaltungs- und Sicherheitsmodell von Active Directory auf und ermöglicht IT-Managern sowie Administratoren auf hoher Ebene eine effiziente Definition und Verteilung von Administratorrechten auf der Grundlage organisatorischer Rollen. Quest One ActiveRoles schließt außerdem eine regelorientierte, automatisierte Bereitstellung anderer IT-Ressourcen ein, die die Verwaltung von Active Directory vereinfacht und verhindert, dass das Verzeichnis mit beschädigten oder inkonsistenten Daten aufgefüllt wird.

Quest One ActiveRolesstellt eine sichere verteilte Verwaltung auf der Grundlage von Unternehmensregeln und -rollen bereit. Dazu werden flexible Rollendefinitionen, die Durchsetzung von Geschäftsregeln, Hilfe bei der Automatisierung sowie eine granuläre Delegierung der Kontrolle über Verzeichnisobjekte kombiniert. Aufbauend auf dem Delegierungsmodell von Active Directory ergänzt das Produkt die Delegationsfunktionen von Active Directory und optimiert die Verwaltung von Delegierungseinstellungen durch Speichern und Anwenden von Rolleninformationen für Administratorfunktionen im Einklang mit Geschäftsregeln des Unternehmens.

Quest One ActiveRoles ist eng in die Funktionalität von Active Directory integriert. Indem das Produkt anpassbare Richtlinien zusammen mit Active Directory-kompatiblen Berechtigungen verwendet, ermöglicht es Administratoren, autorisierten Benutzern eine angemessene Ebene der Kontrolle über Netzwerkressourcen bereitzustellen und administrative Richtlinien einzurichten, die automatisch durchgesetzt und unternehmensweit weitergegeben werden.

Mit Quest One ActiveRoles können Organisationen ihre Netzwerke dynamisch so konfigurieren, dass sowohl eine zentrale als auch eine verteilte Verwaltung von Active Directory als Sammelpunkt der Konfiguration, Verwaltung und Sicherheit von Netzwerkressourcen eingerichtet wird.

Das bietet Quest One ActiveRoles

Quest One ActiveRoles erleichtert die Konten- und Ressourcenverwaltung und -bereitstellung für Active Directory und Exchange. ActiveRoles Server unterstützt Folgendes:

- Durchsetzung von Unternehmensrichtlinien
- Automatisierte Kontobereitstellung
- Rollenbasierte verteilte Verwaltung
- Weitergabe delegierter Rechte an Active Directory
- Sicherheitsverwaltung für Active Directory
- Regelorientierte administrative Ansichten (verwaltete Einheiten)
- Regelbasierte Gruppen (dynamische Gruppen und Gruppenfamilien)
- Genehmigungs-Arbeitsablauf
- Erweiterte Berichterstattung

Durchsetzung von Unternehmensrichtlinien

Im Interesse einer sicheren verteilten Verwaltung müssen administrative Aktionen durch Richtlinien eingeschränkt werden. Quest One ActiveRoles integriert zu diesem Zweck Geschäftsregeln und Verzeichnisaktualisierungen miteinander. Bei jeder Verzeichnisaktualisierung wird eine anpassbare Gruppe von Prozeduren und Richtlinien aufgerufen. Mit dieser Funktion von Quest One ActiveRoles werden die Integrität, Konsistenz und Vollständigkeit der Verzeichnisdaten sichergestellt. Zudem wird Organisationen die Verbesserung ihrer Netzwerksicherheit erleichtert.

Automatisierte Kontobereitstellung

Quest One ActiveRoles stellt umfangreiche Automatisierungsfunktionen für administrative Prozesse bereit. Das Programm ermöglicht die Durchsetzung von Geschäftsregeln durch Ausführung benutzerdefinierter Skripts und Programme vor oder nach bestimmten Tasks und ermöglicht die Verknüpfung mehrerer separater Tasks zu einem einzelnen Vorgang. Diese Möglichkeit, Verwaltungs- und Bereitstellungsaufgaben im Einklang mit Unternehmensrichtlinien zu automatisieren, ist eine der wertvollsten Funktionen von Quest One ActiveRoles.

Rollenbasierte verteilte Verwaltung

Active Directory ermöglicht das Delegieren der administrativen Kontrolle an die Unternehmenseinheiten, die den Zugriff auf bestimmte Verwaltungstasks benötigen. Die Verwaltung einzelner Delegierungseinstellungen ist jedoch zeitaufwändig und fehleranfällig. Quest One ActiveRoles konsolidiert Delegierungsanforderungen mit Hilfe von anpassbaren Administratorfunktionen (Vorlagen), die die geschäftlichen Anforderungen der jeweiligen Organisation erfüllen. Mit Hilfe von Administratorfunktionen erhöht Quest One ActiveRoles die Produktivität der Administratoren und erleichtert die Vermeidung teurer Fehler bei der Verwaltung von Delegierungseinstellungen.

Weitergabe delegierter Rechte an Active Directory

Die in Quest One ActiveRoles angegebenen Rechte für die rollenbasierte Delegierung können an Active Directory weitergegeben werden. Sobald das Weitergeben für die delegierten Berechtigungen festgelegt ist, bleiben sie auch dann synchronisiert, wenn Änderungen in Quest One ActiveRoles vorgenommen werden.

Diese Funktion von Quest One ActiveRoles verbessert die Sicherheit von Active Directory, da sie die Komplexität der Zugriffskontrollverwaltung von Active Directory mit Hilfe der rollenbasierten Delegierung vereinfacht und indem sie Ihnen ermöglicht, präziser und effizienter den Zugriff einzuschränken und die Sicherheit zu bewerten.

Die Möglichkeit, delegierte Rechte an Active Directory weiterzugeben, verbessert die Kontrolle über das Delegierungsmodell von Active Directory. Die entstehende Gruppe von Berechtigungen zeigt die jeweilige Berechtigungsquelle und ermöglicht Ihnen die Ausführung von Berechtigungsüberprüfungen ohne manuelle Analyse des Berechtigungsursprungs. Dies reduziert das Risiko, dass Fehler unterlaufen oder etwas aus Versehen weggelassen wird.

Sicherheitsverwaltung für Active Directory

Die Quest One ActiveRoles-Konsole erleichtert die Untersuchung und Verwaltung von Berechtigungseinträgen in Active Directory und zeigt die den Benutzern zugewiesenen Zugriffsrechte zusammen mit dem Gültigkeitsbereich ihres Zugriffs. Eine zentrale Ansicht der Berechtigungseinträge hilft bei der Analyse und Verwaltung von Berechtigungen in Active Directory. Für jeden Berechtigungseintrag wird in der Ansicht eine Reihe von Eintragseigenschaften einschließlich der Beschreibung, des Ursprungs und des Sicherheitsprinzipals der Berechtigung angezeigt. Zusätzliche Eigenschaften können angezeigt werden, und auf den Editor für die einheitliche Sicherheit kann vom Hauptfenster aus zugegriffen werden.

Auf der Quest One ActiveRoles-Konsole können Sie die Berechtigungen für ein Objekt anzeigen, indem Sie einfach auf das Objekt klicken. Die Berechtigungseinträge werden dann in einer zentralen Ansicht angezeigt. Dies erleichtert Administratoren das Überprüfen der Berechtigungen für sicherheitsrelevante Objekte und das Identifizieren möglicher Sicherheitsprobleme.

Regelorientierte administrative Ansichten (verwaltete Einheiten)

Regelorientierte administrative Ansichten (bezeichnet als verwaltete Einheiten) erleichtern das Anzeigen und Verwalten des Unternehmens, ohne dass die zugrunde liegenden Domänen- und Organisationseinheitsstrukturen verändert werden. Da sie dynamisch an Veränderungen im Unternehmen angepasst werden können, vereinfachen verwaltete Einheiten die Wartung von Geschäftsregeln erheblich. Die Verwendung von verwalteten Einheiten erleichtert die Überwindung der Beschränkungen, die starren Organisationsstrukturen innewohnen, und entspricht der Anforderung, die Verwaltung außerhalb der Grenzen von Organisationseinheit, Domäne und Gesamtstruktur auszuführen.

Regelorientierte Gruppen (dynamische Gruppen)

Quest One ActiveRoles ermöglicht es, Gruppenmitgliedschaftslisten automatisch aktuell zu halten, sodass Sie Mitglieder nicht manuell hinzufügen und entfernen müssen. Die regelorientierte Verwaltung von Mitgliedschaftslisten verringert die Wartungskosten für Gruppen. Außerdem erhöht sie die Genauigkeit und Zuverlässigkeit der Nachrichtenverteilung über die Mitgliedschaft in Verteilergruppen sowie die Konsistenz von Sicherheitseinstellungen über die Mitgliedschaft in Sicherheitsgruppen.

Regelorientierte Gruppenfamilien

Quest One ActiveRoles stellt eine neue Kategorie regelorientierter Richtlinien für die automatische Gruppenbereitstellung bereit. Jede Richtlinie dieser Kategorie, die als Gruppenfamilie bezeichnet wird, dient als Kontrollmechanismus für die Erstellung und Auffüllung von Gruppen. Diese neuen Richtlinien sollen die bei der Verwaltung der Gruppenmitgliedschaft auftretenden Probleme lösen.

Die Gruppenfamilie erstellt automatisch Gruppen und pflegt Gruppenmitgliedschaftslisten. Dabei hält sie konfigurierbare Regeln ein. Die Gruppenmitgliedschaft kann somit anhand von Objekteigenschaften im Verzeichnis definiert werden. Die Gruppenfamilie ermöglicht außerdem die Erstellung neuer Gruppen anhand neuer Werte, die in Objekteigenschaften erkannt werden.

Die Konfiguration einer Gruppenfamilie muss nicht auf eine einzelne Objekteigenschaft beschränkt sein. Sie kann aus so vielen Eigenschaften kombiniert werden wie nötig. Beispielsweise kann eine Gruppenfamilie so eingerichtet werden, dass sie die Eigenschaften „Abteilung" und „Stadt" berücksichtigt. Folglich erstellt und pflegt die Gruppenfamilie eine separate Gruppe für jede Abteilung an jedem geografischen Standort.

Genehmigungs-Arbeitsablauf

Quest One ActiveRoles bietet in seinem Modul „Regeln & Rollen" Genehmigungs-Arbeitsablauffunktionen. Durch die Bereitstellung einer regelbasierten, anpassbaren Genehmigungsweiterleitung verringert Quest One ActiveRoles Fehler und Inkonsistenzen bei der Verwaltung von Verzeichnisdaten. Während automatisierte Richtlinien keinen manuellen Eingriff erfordern, erweitert die auf Genehmigungen basierende Durchführung administrativer Vorgänge die Prozessautomatisierung um die Möglichkeit, angeforderte Vorgänge manuell zu genehmigen oder abzulehnen und die Ausführung von Genehmigungsaufgaben zu überwachen, um zu gewährleisten, dass diese zeitnah beantwortet werden.

Der Genehmigungs-Arbeitsablauf ist nützlich für eine Reihe von Benutzerverwaltungsaufgaben wie etwa die Erstellung, das Löschen und die Änderung von Objekten sowie die Bereitstellung und Deprovision von Benutzerkonten. Die Vorgänge können durch festgelegte Benutzer über das Quest One ActiveRoles Web-Interface initiiert werden.

Wenn ein angeforderter Vorgang die Berechtigung durch bestimmte Personen in einer Organisation erfordert, koordiniert ein Arbeitsablauf den Genehmigungsprozess. Das System führt den angeforderten Vorgang erst durch, wenn eine autorisierte Person die entsprechende Genehmigung erteilt hat.

Um den Genehmigungs-Arbeitsablauf zu konfigurieren, erstellt der Administrator Genehmigungsregeln mit Hilfe der Quest One ActiveRoles-Konsole. Genehmigungsregeln werden verwendet, um die Vorgänge anzugeben, die Gegenstand einer Genehmigung sind, und um die Personen festzulegen, die autorisiert sind, Genehmigungsaufgaben durchzuführen.

Erweiterte Berichterstattung

Quest One ActiveRoles verfügt über erweiterte Berichterstattungsfunktionen, mit denen alle administrativen Aktionen protokolliert und überprüft werden können. Das Berichterstattungspaket von Quest One ActiveRoles enthält zahlreiche vordefinierte Berichte, die alle möglichen administrativen Aktionen abdecken. Viele dieser Berichte sind anpassbar, sodass der Administrator den Berichtsinhalt steuern kann. Außerdem stellt Quest One ActiveRoles leicht zu verwendende Tools zum Erstellen beliebig vieler benutzerdefinierter Berichte bereit, in denen spezifische Daten wie beispielsweise der Zustands- und Änderungsverlauf eines Objekts isoliert dargestellt werden können.

Warum Quest One ActiveRoles?

Heute verlassen sich Organisationen zunehmend auf Active Directory und betrachten Active Directory als unternehmenswichtige Anwendung in ihrer Umgebung. Daher ist es wichtig, die mit Active Directory interagierenden Geschäftsprozesse zu steuern. Dies muss so sicher, so gut kontrolliert und so effizient wie möglich erfolgen. Quest One ActiveRoles ermöglicht die vollständige Steuerung der Verzeichnisverwaltung über die rollenbasierte Sicherheit und die regelorientierte Automatisierung der Tasks für die Bereitstellung, erneute Bereitstellung und Deprovisionierung in Active Directory, Exchange und Windows. Das Programm bietet eine umfassende Lösung, die die Verwaltung vereinfacht, die Sicherheit verbessert und die Produktivität der Administratoren erhöht.

Automatisierte Bereitstellung für Benutzer

Quest One ActiveRoles automatisiert die Aufgaben der Bereitstellung für Benutzer, verringert so Ihre Arbeitslast für die Verwaltung und ermöglicht es, neuen Benutzern schneller die benötigten Ressourcen bereitzustellen. Das Programm automatisiert außerdem auch die erneute Bereitstellung und die Deprovision. Wenn der Zugriff eines Benutzers geändert oder entfernt werden muss, werden Aktualisierungen in Active Directory, Exchange und Windows also automatisch vorgenommen. Dies reduziert die Arbeitslast für die Verwaltung und ermöglicht Benutzern eine schnellere, größere Produktivität.

Vereinfachte Verwaltung

Quest One ActiveRoles ist einfach zu installieren, bereitzustellen und zu verwenden und ermöglicht den dafür ausgewählten Personen die schnelle und leichte Ausführung von Verwaltungsaufgaben. Dank der umfangreichen Integrationsfunktionen werden komplexe Aufgaben erleichtert und gegen Fehler abgesichert. Da administrative Richtlinien des Unternehmens durchgesetzt werden können, wird sichergestellt, dass der Sicherheitsentwurf und die Vorgehensweisen für den Betrieb unabhängig davon befolgt werden, welcher Administrator die Verwaltungsaufgaben ausführt. Quest One ActiveRoles vereinfacht die Verwaltung, sodass auch weniger umfassende Fähigkeiten ausreichen, um die Windows-Unternehmensinfrastruktur zu administrieren.

Quest One ActiveRoles stellt intuitiv verständliche, vereinheitlichte Benutzeroberflächen bereit, über die auch Mitarbeiter mit begrenzter Verwaltungserfahrung Netzwerkbenutzer, Gruppen und Computer verwalten können. Mit Quest One ActiveRoles können regelmäßige Verwaltungsaufgaben unter Wahrung der Sicherheit an abteilungsinterne Administratoren und an Help Desk-Operatoren delegiert werden, selbst wenn diese nur über grundlegendes Wissen verfügen.

Verbesserte Sicherheit

Quest One ActiveRoles ergänzt das Sicherheitsmodell von Active Directory und stellt sicher, dass die Genauigkeit der Verzeichnisdaten anhand administrativer Richtlinien des Unternehmens aufrechterhalten wird. Die Richtliniendurchsetzung dieses Produkts stellt sicher, dass jede administrative Aktion den Sicherheitsstandards des Unternehmens entspricht. Dies hat für die meisten Organisationen höchste Priorität.

Mit Quest One ActiveRoles können Verwaltungsaufgaben auf sichere Weise an die passenden Personen delegiert werden. Das Programm stellt eine richtlinienbasierte, kontrollierte Umgebung bereit, in der autorisierte Benutzer mit Verzeichnisdatenquellen interagieren können, und stellt konsistente Ebenen von Administratorrechten, eine verbesserte Sicherheit sowie eine vereinfachte Verwaltung der Verzeichnisdaten sicher.

Alle Aktivitäten von Quest One ActiveRoles werden in einem separaten Ereignisprotokoll aufgezeichnet. Diese detaillierten Protokolleinträge ermöglichen die schnelle Identifikation und Verwaltung potenzieller Sicherheitsprobleme. Quest One ActiveRoles stellt ein vollständiges Prüfprotokoll bereit. Dieses zeigt alle ausgeführten Aktionen und ihre Urheber sowie auch Aktionen, die nicht zugelassen wurden. Durch eine Analyse des Prüfprotokolls können Sie Sicherheitsbedrohungen erkennen und Sicherheitsprobleme verhindern.

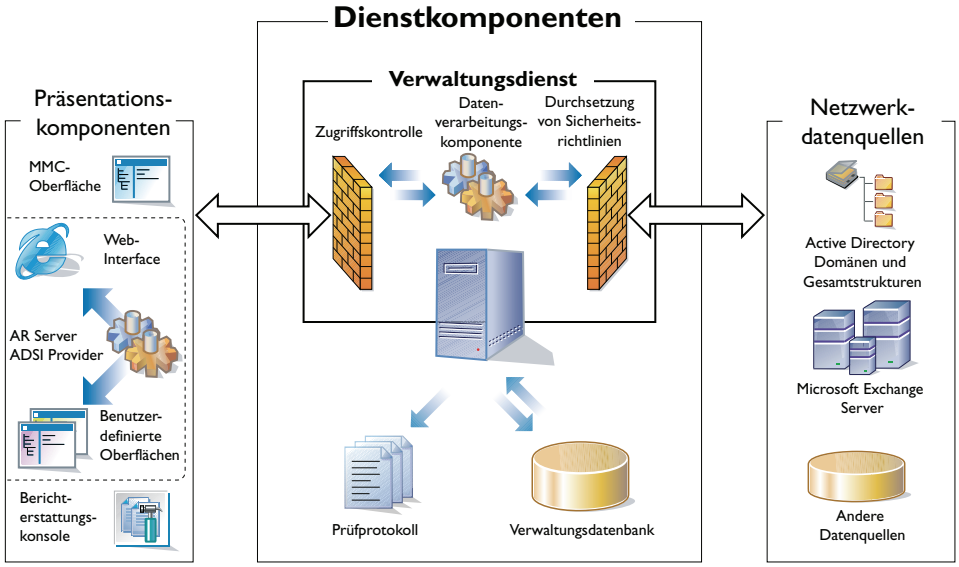
Erhöhte Produktivität

Quest One ActiveRoles erhöht die Produktivität der Verzeichnisadministratoren und Help Desk-Operatoren durch Automatisieren der Bereitstellungsaufgaben wie das Erstellen von Exchange-Postfächern, das Zuweisen von Stammordnern und das Warten von Gruppen. Ebenfalls vorhanden sind umfangreiche Skriptfunktionen, die eine flexible Automatisierungsmöglichkeit für Verwaltungsvorgänge bereitstellen und mit denen Active Directory und Exchange in andere Geschäftsprozesse integriert werden können. Dank der anpassbaren Integration und der Automatisierung von Verwaltungsaufgaben erhöht Quest One ActiveRoles die Produktivität und hilft bei der Vermeidung teurer Fehler.

Die von Quest One ActiveRoles bereitgestellte automatisierte Richtliniendurchsetzung stellt sicher, dass Unternehmensrichtlinien konsistent befolgt werden, unabhängig davon, welche Person administrative Aktionen ausführt. Durch die Verteilung und Automatisierung regelmäßiger Verwaltungsaufgaben ermöglicht Quest One ActiveRoles es Verzeichnisadministratoren, sich auf strategische Vorhaben wie die Planung des Verzeichnisses, die Erhöhung der Unternehmenssicherheit oder die Unterstützung unternehmenswichtiger Anwendungen zu konzentrieren.

Technische Übersicht

Quest One ActiveRoles teilt die Arbeitsauslastung für die Directory-Verwaltung und -Bereitstellung in drei Funktionsebenen—Präsentationskomponenten, Dienstkomponenten und Netzwerkdatenquellen.



Zu den Präsentationskomponenten gehören Clientbenutzeroberflächen für die Windows-Plattform und das Web, mit denen gewöhnliche Benutzer einen genau definierten Satz administrativer Aktionen ausführen können. Die Berichterstattungslösung erleichtert das automatisierte Generieren von Berichten zu Verwaltungsaktivitäten.

Die Dienstkomponenten stellen eine geschützte Ebene zwischen Administratoren und verwalteten Datenquellen dar. Diese Ebene stellt eine konsistente Durchsetzung von Richtlinien sicher, stellt erweiterte Automatisierungsfunktionen bereit und ermöglicht die Integration von Geschäftsprozessen für die Verwaltung von Active Directory, Microsoft Exchange und anderen Datenquellen im Unternehmen.

Die Verwaltungsdatenbank speichert Informationen über alle Berechtigungs- und Richtlinieneinstellungen sowie sonstige Daten im Zusammenhang mit der Quest One ActiveRoles-Konfiguration.

Auf einer sehr hohen Ebene arbeiten die Quest One ActiveRoles-Komponenten wie folgt zusammen, um die Directory-Daten zu bearbeiten:

1. Ein Administrator verwendet die MMC- oder Web-Schnittstelle, um auf Quest One ActiveRoles zuzugreifen.
2. Der Administrator übersendet eine Vorgangsanforderung, z.B. eine Abfrage oder eine Datenänderung, an den Verwaltungsdienst.
3. Bei Erhalt der Vorgangsanforderung überprüft der Verwaltungsdienst, ob der Administrator über hinreichende Berechtigungen zum Ausführen des angeforderten Vorgangs verfügt (Zugriffsprüfung).
4. Der Verwaltungsdienst stellt sicher, dass der angeforderte Vorgang die Unternehmensrichtlinien nicht verletzt (Richtliniendurchsetzung).
5. Der Verwaltungsdienst führt alle aufgrund von Unternehmensrichtlinien erforderlichen Aktionen aus, bevor er die Anforderung zur Verarbeitung freigibt (Richtliniendurchsetzung).

6. Der Verwaltungsdienst gibt Aufrufe von Betriebssystemfunktionen aus, um den angeforderten Vorgang für Netzwerkdatenquellen auszuführen.
7. Der Verwaltungsdienst führt nach der Verarbeitung der Anforderung durch das Betriebssystem alle zugehörigen Aktionen aus, die aufgrund der Unternehmensrichtlinien erforderlich sind (Richtliniendurchsetzung).
8. Der Verwaltungsdienst generiert einen Audit-Trail, der Datensätze über alle ausgeführten oder mit Quest One ActiveRoles versuchten Vorgängen beinhaltet. Nachverfolgungsberichte für Verzeichnisänderungen basieren auf dem Prüfprotokoll.

Im Folgenden werden die drei Komponentenebenen betrachtet.

Präsentationskomponenten

Zu den Präsentationskomponenten gehören Benutzeroberflächen, die eine Vielzahl von Anforderungen erfüllen. Die Benutzeroberfläche akzeptiert Befehle, zeigt Kommunikationsdaten an und präsentiert Ergebnisse auf klare, prägnante Weise.

Quest One ActiveRoles Konsole (MMC-Schnittstelle)

Die Quest One ActiveRoles-Konsole, die auch als MMC-Schnittstelle bezeichnet wird, ist ein umfassendes Verwaltungstool für Active Directory und Microsoft Exchange. Sie ermöglicht das Festlegen von Administratorfunktionen und das Delegieren der Kontrolle, das Definieren von administrativen Richtlinien und Automatisierungsskripts, das einfache Finden von Verzeichnisobjekten und die Ausführung von Verwaltungsaufgaben.

Web-Interface

Über die Webschnittstelle können Intranet-Benutzer mit ausreichenden Verwaltungsberechtigungen die Verbindung mit Quest One ActiveRoles herstellen, um einfache Verwaltungsaufgaben auszuführen, z.B. Benutzerdaten ändern oder Benutzer in Gruppen hinzufügen. Das Web-Interface stellt Mitarbeitern der Abteilungen und des Help Desk die Verwaltungsfunktionen bereit, die sie benötigen.

Benutzerdefinierte Benutzeroberflächen

Abgesehen von der MMC- und Web-Schnittstelle ermöglicht Quest One ActiveRoles die Entwicklung benutzerdefinierter Schnittstellen, die den Quest One ActiveRoles ADSI-Provider für den Zugriff auf die Funktionen zu Quest One ActiveRoles. Administratoren mit Kenntnissen der Skripterstellung und Programmierung können benutzerdefinierte Benutzeroberflächen erstellen, die die spezifischen Anforderungen für die Netzwerkverwaltung erfüllen.

Quest One ActiveRoles ADSI Provider

Der Quest One ActiveRoles ADSI-Provider fungiert als Teil der Präsentationskomponenten, um benutzerdefinierten Benutzerschnittstellen und -anwendungen den Zugriff auf Active-Directory-Dienst durch Quest One ActiveRoles zu ermöglichen. Der Quest One ActiveRoles ADSI Provider übersetzt die Client-Anforderungen in DCOM-Anrufe und wirkt mit dem Verwaltungsdienst zusammen.

Der Quest One ActiveRoles ADSI Provider ermöglicht es benutzerdefinierten Skripts und Anwendungen, z.B. Web-basierten Anwendungen, mit Active Directory zu kommunizieren und dabei die Sicherheit, die Workflow-Integration und die Berichtserstellungsvorteile von Quest One ActiveRoles voll auszuschöpfen. Beispielsweise können mit Hilfe von Quest One ActiveRoles ADSI Provider Web-bassierte Seiten erstellt werden, so dass von Help-Desk-Operatorenvorgenommene Eigenschaftsänderungen durch die von Quest One ActiveRoles erzwungenen Geschäftsregeln beschränkt werden.

Berichtslösung

Quest One ActiveRoles bietet umfassende Berichtserstellung, um die administrativen Vorgänge, die Einhaltung firmeninterner Richtlinien und den Status von Directory-Objekten zu überwachen. Die Quest One ActiveRoles Berichterstellungslösung beinhaltet das Datensammler- und Berichts-Paket.

Das Berichtspaket Report Pack stellt Berichtsdefinitionen für die Erstellung von Berichten auf Grundlage der vom Data Collector gesammelten Daten. Quest One ActiveRoles wird mit einer umfassenden Sammlung von Berichtsdefinitionen geliefert, die alle in diesem Projekt verfügbaren Verwaltungsvorgänge abdecken.

Report Pack erfordert Microsoft SQL Server Reporting Services (SSRS). Sie können die in SSRS enthaltenen Tools verwenden, um Quest One ActiveRoles-Berichte einzusehen, zu speichern, auszudrucken, zu veröffentlichen und zu programmieren.

Data Collector wird für die Erfassung der für die Berichterstattung erforderlichen Daten verwendet. Der Data Collector-Assistent ermöglicht Ihnen, Datenerfassungsaufträge zu konfigurieren und zu planen.

Nach erfolgter Konfiguration ruft der Data Collector Daten aus unterschiedlichen Quellen ab, indem er über den Quest One ActiveRoles-Verwaltungsdienst darauf zugrifft, und speichert die Daten in einer SQL-Server-Datenbank. Data Collector stellt außerdem ein Mittel für die Verwaltung der erfassten Daten dar und bietet darüber hinaus die Möglichkeit, veraltete Daten zu exportieren oder zu löschen.

Dienstkomponenten

Im Kern von Quest One ActiveRoles liegt der Verwaltungsdienst. Er enthält erweiterte Delegationsfunktionen und gewährleistet die zuverlässige Durchsetzung administrativer Richtlinien, mit denen Daten aktuell und genau gehalten werden. Der Verwaltungsdienst fungiert als eine Art Brücke zwischen den Präsentationskomponenten und den Netzwerk-Datenquellen. In großen Netzwerken können mehrere Verwaltungsdienste bereitgestellt werden, um die Leistung zu steigern und um eine Fehlertoleranz zu gewährleisten.

Datenverarbeitungskomponente

Die Datenverarbeitungskomponente akzeptiert administrative Anforderung und validiert sie, indem sie die in der Verwaltungsdatenbank gespeicherten Berechtigungen und Regeln überprüft. Diese Komponente verwaltet die Netzwerkdatenquellen. Anhand von administrativen Anforderungen und Richtliniendefinitionen ruft sie die entsprechenden Netzwerkobjektdaten ab oder ändert sie.

Die Datenverarbeitungskomponente fungiert als ein sicherer Dienst. Er meldet sich mit Domänenbenutzerkonten an, die über ausreichende Privilegien verfügen, um Zugriff auf die mit Quest One ActiveRoles registrierten Domänen (verwaltete Domänen) zu erlangen. Der Zugriff auf die verwalteten Domänen wird durch die Zugriffsrechte dieser Benutzerkonten eingeschränkt.

Konfigurationsdatenbank

Der Verwaltungsdienst verwendet die Konfigurationsdatenbank (die auch als Verwaltungsdatenbank bezeichnet wird) für die Speicherung von Konfigurationsdaten. Die Konfigurationsdaten schließen für Quest One ActiveRoles spezifische Objekte, Zuweisungen von Verwaltungsrollen und -richtlinien sowie Verfahren ein, die für die Richtlinienerzwingung verwendet werden. Die Verwaltungsdatenbank wird nur verwendet, um die Quest One ActiveRoles-Konfigurationsdaten zu speichern. Sie speichert keine Kopien der Objekte, die sich in den verwalteten Datenquellen befinden, noch wird sie als ein Objektdaten-Zwischenspeicher verwendet.

Quest One ActiveRoles verwendet den Microsoft SQL Server, um die Konfigurationsdatenbank zu beherbergen. Die Replikationsfunktionen von SQL Server erleichtern die Implementierung von mehreren äquivalenten Konfigurationsdatenbanken, die von verschiedenen Verwaltungsdiensten verwendet werden.

Prüfprotokoll

Die Datenverarbeitungskomponente bietet einen umfassenden Audit Trail, indem sie Einträge im Ereignisprotokoll auf dem Computer erstellt, auf dem der Verwaltungsdienst ausgeführt wird. Das Protokoll zeigt alle ausgeführten Aktionen und ihre Urheber sowie Aktionen, die nicht zugelassen wurden. Die Protokolleinträge zeigen den Erfolg oder Fehler jeder Aktion sowie die geänderten Attribute an.

Netzwerkdatenquellen

Durch den Verwaltungsdienst greift Quest One ActiveRoles auf die in den folgenden Datenquellen gespeicherten Objektdaten zu und kontrolliert sie:

- **Active Directory-Domänen & Gesamtstrukturen.** Stellt die Verzeichnisobjektinformationen in Active Directory-Domänen bereit.
- **Microsoft Exchange Server.** Stellt Informationen zu Postfächern bereit, die von Microsoft Exchange verwaltet werden.
- **Andere Datenquellen.** Stellt Informationen über außerhalb von Active Directory existierende Objekte bereit. Hierzu gehören Informationen aus Unternehmensdatenbanken wie etwa die Datenbank der Personalabteilung und Informationen über Computerressourcen wie etwa Dienste, Drucker und Netzwerkdateifreigaben.

Quest One ActiveRoles wurde entwickelt, um die Verwendung und Verwaltung dieser Datenquellen zu unterstützen. Verzeichnisadministratoren können Geschäftsregeln und Geschäftsrichtlinien definieren und durchsetzen, um sicherzustellen, dass die Daten in den verwalteten Datenquellen aktuell und genau bleiben.

Mit Quest One ActiveRoles können Sie die Informationsspeicher aus einer großen Anzahl von Datenquellen in Ihrem Netzwerk verwenden, z.B. Personaldaten oder Lagerbestände. Sie können die Skripterstellung für die Integration dieser wichtigen Datenquellen verwenden. Dies verringert doppelte Arbeiten und die Datenverfälschung und ermöglicht die Auswertung von Informationen, die häufig in mehr als einer Datenbank gespeichert werden.

Quest One ActiveRoles ermöglicht es einem benutzerdefinierten Skript, Kontrolle über eine Anforderung, einen Verwaltungsvorgang auszuführen, zu erlangen, z.B. Erstellung, Änderung oder Löschung eines Objekts. Benutzerdefinierte Skripts können durch Richtlinienobjekte aufgerufen werden, welche Quest One ActiveRoles verwendet, um firmeninterne Richtlinien zu erzwingen. Beispielsweise könnten Sie ein Richtlinienobjekt implementieren, das ein benutzerdefiniertes Skript enthält, welches Kontrolle erlangt, wann immer Quest One ActiveRoles angefordert wird, um ein Benutzerobjekt in einer bestimmten Organisationseinheit zu erstellen.

Das Richtlinienobjekt könnte so konfiguriert werden, dass Quest One ActiveRoles mit der Benutzererstellung erst weitermacht, wenn ein bestimmtes Element des Skripts (der Vorbereitungs-Ereignishandler) erfolgreich ausgeführt wurde. Auf diese Weise verhindert das Skript die Erstellung von Benutzerobjekten, deren Eigenschaften gegen Unternehmensregeln verstoßen. Es verhindert das Füllen von Objekteigenschaften mit Werten, die aus externen Datenquellen stammen, und generiert Standard-Eigenschaftswerte in Übereinstimmung mit den Unternehmensregeln.

Das Richtlinienobjekt kann auch so konfiguriert werden, dass die Kontrolle unmittelbar nach erfolgreicher Erstellung eines Benutzerobjekts an einen anderen Teil des Skripts übergeben wird (dernach der Erstellung eingesetzte Ereignis-Handler). Dies ermöglicht dem Skript, zusätzliche, von Unternehmensregeln geforderte Vorgänge auszulösen, nachdem das Objekt erstellt wurde. So kann es zum Beispiel externe Datenspeicher aktualisieren, dem Benutzer einen Zugriff auf Ressourcen bereitstellen und über die Erstellung des Benutzerobjekts informieren.

Sicherheits- und Verwaltungselemente

Quest One ActiveRoles bietet drei vorrangige Sicherheits- und Verwaltungselemente, die als Objekte in der Verwaltungsdatenbank gespeichert werden:

- Zugriffsvorlagen
- Richtlinienobjekte
- Verwaltete Einheiten

Diese Elemente ermöglichen es, jedem Benutzer oder jeder Gruppe in Active Directory eingeschränkte und effektiv kontrollierte administrative Rechte zu gewähren.

Die Benutzer und Gruppen, die in Quest One ActiveRoles administrative Berechtigungen erhalten, werden als *Vertrauensnehmer* bezeichnet. Trustees können verwalteten Einheiten oder Verzeichnisobjekten und Containern zugewiesen werden.

Trustees haben keine speziellen administrativen Rechte innerhalb von Active Directory. Um den Vertrauensnehmern den Zugriff auf Active Directory zu erteilen, implementiert Quest One ActiveRoles Proxymechanismen, die Access-Vorlagen verwenden, um die Zugangsebene festzulegen. Wenn Trustees ihre Zugriffsberechtigungen wahrnehmen, verwenden diese Mechanismen Richtlinienobjekte für die Auslösung weiterer Vorgänge wie etwa die Ausführung von Integrationsskripts und die Validierung von Eingangsdaten.

Wenn Sie einen Benutzer oder eine Gruppe zu einem Trustee ernennen, müssen Sie die Zugriffsvorlagen angeben, die kontrollieren, zu welchen Vorgängen der Trustee berechtigt ist. Einer Gruppe gewährte Berechtigungen gelten für alle Mitglieder dieser Gruppe. Um den Verwaltungsaufwand zu reduzieren, sollte die administrative Kontrolle an Gruppen und nicht an einzelne Benutzer delegiert werden.

Um Richtlinieneinschränkungen und eine Automatisierung zu implementieren, müssen Sie Richtlinienobjekte konfigurieren und anwenden, die bei administrativen Anforderungen integrierte oder benutzerdefinierte Verfahren aufrufen. Richtlinienverfahren können die Ausführung von benutzerdefinierten Skripts für die Synchronisation von Active Directory-Daten mit anderen Datenquellen, die Durchführung einer Datengültigkeitsprüfung und den Start weiterer administrativer Vorgänge umfassen.

Zugriffsvorlagen für die rollenbasierte Administration

Eine *Access-Vorlage* ist eine Sammlung von Berechtigungen, die festlegen, welche Vorgänge von einer administrativen Rolle ausgeführt werden können. Quest One ActiveRoles wendet Access-Vorlagen auf Directory-Objekte, Container und administrative Ansichten (verwaltete Einheiten) im Zusammenhang mit als Vertrauensnehmer bezeichneten Gruppen und Benutzern an.

Quest One ActiveRoles bietet eine umfangreiche Sammlung vorkonfigurierter Access-Vorlagen, die typische Verwaltungsrollen darstellen, welche die rasche und konsistente Delegierung der korrekten Ebene der Verwaltungsautorität ermöglichen. Zugriffsvorlagen vereinfachen in erheblichem Maß die Delegation und Verwaltung von administrativen Rechten, beschleunigen die Bereitstellung des Delegationsmodells und verringern die Verwaltungskosten. Die vorkonfigurierten Access-Vorlagen werden im „out of the box" verfügbaren *Quest One ActiveRoles Access-Templates*-Dokument besprochen.

Zugriffsvorlagen ermöglichen zentralisierten Administratoren die Definition von Administratorfunktionen mit verschiedenen Berechtigungsebenen, wodurch die Bereitstellung einer Zugriffskontrolle beschleunigt und die Verfolgung von Änderungen an Berechtigungseinstellungen im gesamten Unternehmen rationalisiert wird.

Es ist auch möglich, benutzerdefinierte Zugriffsvorlagen auf der Grundlage von Businessanforderungen zu erstellen. Benutzerdefinierte Zugriffsvorlagen können jederzeit geändert werden. Wenn eine Zugriffsvorlage geändert wird, ändern sich die Berechtigungseinstellungen für alle Objekte, auf die diese Zugriffsvorlage angewandt wird, entsprechend.

Richtlinienobjekte zur Erzwingung von Unternehmensregeln

Ein *Richtlinienobjekt* ist eine Sammlung administrativer Richtliniendefinitionen, die durchzusetzende Unternehmensregeln angeben. Die Access-Vorlagen legen fest, wer Änderungen an einem Datenelement vornehmen kann, und die Richtlinienobjekte kontrollieren, welche Änderungen an den Daten vorgenommen werden können. Quest One ActiveRoles erzwingt Firmenrichtlinien durch Verknüpfung der Policy-Objekte mit:

- Administrative Ansichten (verwaltete Einheiten)
- Active Directory-Container
- Individuelle Verzeichnisobjekte

Richtlinienobjekte definieren das Verhalten des Systems bei der Erstellung oder Änderung, beim Verschieben oder beim Löschen von Verzeichnisobjekten. Richtlinien werden unabhängig von den Berechtigungen eines Trustees erzwungen.

Ein Richtlinienobjekt schließt gespeicherte Richtlinienprozeduren und Angaben von Ereignissen ein, die die jeweilige Prozedur aktivieren. Auf der Grundlage von Richtlinienanforderungen kann ein Richtlinienverfahren folgende Aktionen durchführen:

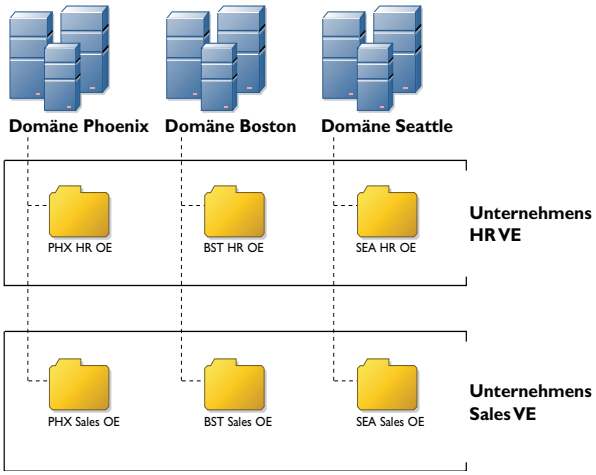
- Validieren von spezifischen Eigenschaftswerten
- Zulassen oder Verweigern von ganzen Vorgängen
- Auslösen weiterer Vorgänge

Ein Richtlinienobjekt ordnet seinen Richtlinienprozeduren spezifische Ereignisse zu, bei denen es sich um integrierte Prozeduren oder benutzerdefinierte Skripts handeln kann. Dies ermöglicht die einfache Implementierung komplexer Überprüfungskriterien, die Synchronisierung verschiedener Datenquellen und die Kombination einer Reihe von Verwaltungstasks in einem einzelnen Batch.

Verwaltete Einheiten für die Bereitstellung administrativer Ansichten

Eine *verwaltete Einheit* ist eine Sammlung von kollektiv mit Quest One ActiveRoles verwalteten Objekten, die zur Verteilung administrativer Verantwortungen, Erzwingung von Firmenrichtlinien und Geschäftsstandards erstellt wurden, und dem Management komplexer Netzwerkumgebungen. Mit Hilfe von verwalteten Einheiten kann das Verwaltungsgerüst vom Active Directory-Design getrennt werden. Verzeichnisobjekte können unabhängig vom Speicherort des Objekts in Active Directory einfach in administrativen Ansichten zusammengefasst werden.

So kann das Active Directory-Design zum Beispiel auf dem geografischen Standort beruhen, wobei Domänen nach Städten oder Regionen und Organisationseinheiten nach Unternehmensabteilungen oder gruppen benannt werden. Verwaltete Einheiten können jedoch auch so gestaltet werden, dass spezifische Abteilungen oder Gruppen verwaltet werden, die auf mehrere geografische Standorte aufgeteilt sind.



In diesem Beispiel hat jede AD-Domäne eine „Human Resources" (HR) -Organisationseinheit und eine „Sales"-Organisationseinheit. Quest One ActiveRoles verfugt uber eine verwaltete Einheit („MU") für das „Personalwesen" und eine für den „Verkauf". Die verwaltete Einheit „HR" ermöglicht es den Administratoren, die für alle HR-Benutzer erforderlichen Richtlinien und Sicherheitseinschränkungen unabhängig von deren Standort zu konfigurieren, während die verwaltete Einheit „Sales" dieselbe Funktion für alle Sales-Benutzer bietet.

Die verwalteten Einheiten werden durch die Verwendung von Mitgliedschaftsregeln festgelegt—von Quest One ActiveRoles verwendeten Kriterien, um zu beurteilen, ob ein Objekt zu einer vorgegebenen verwalteten Einheit gehört oder nicht. Dies ermöglicht die dynamische Änderung von verwalteten Einheiten, wenn sich die Netzwerkumgebung ändert. Sie können zum Beispiel eine verwaltete Einheit definieren, indem Sie Regeln angeben, die alle Objekte umfassen, deren Eigenschaften mit bestimmten Bedingungen übereinstimmen. Die angegebenen Regeln zwingen die neuen oder geänderten Objekte, Mitglieder der richtigen verwalteten Einheit zu sein.

Verwaltete Einheiten erweitern die Funktion von Organisationseinheiten, indem Sie einen bequemen Bereich für die Delegation der Verwaltung und die Erzwingung von Unternehmensregeln bieten. Eine verwaltete Einheit weist die folgenden Merkmale auf:

- Repräsentiert eine Sammlung aus Objekten (ein Objekt kann mehr als einer verwalteten Einheit angehören)

- Sie unterstützt regelbasierte Spezifikationen für ihre Mitglieder (eine verwaltete Einheit enthält nur Objekte, die den für die verwaltete Einheit angegebenen Mitgliedschaftsregeln entsprechen)
- Sie kann Verzeichnisobjekte enthalten, die sich in verschiedenen Organisationseinheiten, Domänen, Gesamtstrukturen und anderen verwalteten Einheiten befinden

Quest One ActiveRoles stellt sicher, dass die für eine verwaltete Einheit angegebenen Berechtigungs- und Richtlinieneinstellungen an alle Objekten, die zu dieser verwaltete Einheit gehörten, vererbt werden. Wenn ein Verzeichniscontainer zu einer verwalteten Einheit gehört, erben alle untergeordneten Objekte in diesem Container die auf der Ebene der verwalteten Einheit definierten Berechtigungs- und Richtlinieneinstellungen. Diese Vererbung setzt sich die gesamte Verzeichnisstruktur innerhalb aller Containerobjekte, die Mitglieder der verwalteten Einheit sind, nach unten fort.

Sicherheitsverwaltung für Active Directory

Die Quest One ActiveRoles MMC-Schnittstelle macht es einfach, Berechtigungseinträge im Active Directory zu untersuchen und zu verwalten, indem der für jeden Benutzer verfügbare Zugriff zusammen mit dem Umfang des jeweiligen Zugriffs gezeigt wird. Eine zentrale Ansicht aller Berechtigungseinträge für ein bestimmtes Objekt unterstützt die Analyse und Verwaltung von Berechtigungen in Active Directory. Für jeden Berechtigungseintrag wird in der Ansicht eine Reihe von Eintragseigenschaften einschließlich der Beschreibung, des Ursprungs und des Sicherheitsprinzipals der Berechtigung angezeigt. Ausgehend vom Hauptfenster können Zusätzliche Eigenschaften angezeigt werden. Außerdem kann auf den Editor für die einheitliche Sicherheit zugegriffen werden.

Die zentralisierte Anzeige der einheitlichen Sicherheit ermöglicht es dem Administrator, schnell die Berechtigungen einzusehen, die Objekten in Active Directory zugewiesen sind, und zu ermitteln, ob die Berechtigung übernommen wurde oder nicht. Die Liste der Berechtigungseinträge kann nach dem Sicherheitsprinzipalnamen sortiert werden, um zu ermitteln, wer Zugriff auf das ausgewählte Objekt hat. Wenn ein Berechtigungseintrag vererbt wird, identifiziert Quest One ActiveRoles das Objekt, von welchem die Berechtigung stammt, so dass der Administrator den Berechtigungseintrag für dieses Objekt leicht finden und bearbeiten kann.

Die Quest One ActiveRoles MMC-Schnittstelle bietet die Möglichkeit, die Berechtigungen für ein Objekt durch einfaches Anklicken des Objekts einzusehen, um die Berechtigungseinträge in einer zentralen Ansicht darzustellen. Dies erleichtert Administratoren das Überprüfen der Berechtigungen für sicherheitsrelevante Objekte und das Identifizieren möglicher Sicherheitsprobleme.

Verwaltung der einheitlichen Sicherheit

Quest One ActiveRoles Die Access-Vorlagen können verwendet werden, um die Berechtigungen in Active Directory anzugeben. Die für die Unterstützung der rollenbasierten Gruppierung von Berechtigungen konzipierten Zugriffsvorlagen bieten einen effizienten Mechanismus für die Einstellung und Aufrechterhaltung der Zugriffskontrolle, wodurch die Verwaltung von Berechtigungen in Active Directory vereinfacht und verbessert wird.

Um diese Möglichkeit zu bieten, erteilt Quest One ActiveRoles dem Administrator die Option, die systemeigene Sicherheit mit ausgewählten Berechtigungen, die mit Hilfe von Access-Vorlagen angegeben werden, aktualisiert zu halten. Diese Option, die als „Weitergabe von Berechtigungen" bezeichnet wird, soll Benutzern und Anwendungen einheitliche Berechtigungen für Active Directory bereitstellen. Der normale Vorgang von Quest One ActiveRoles beruht nicht auf dieser Option.

Für Quest One ActiveRoles Berechtigungseinträge mit Berechtigungspropagierungs-Optionssatz generiert Quest One ActiveRoles systemeigene Active Directory-Berechtigungseinträge gemäß den Quest One ActiveRoles-Berechtigungen. Nachdem die Option festgelegt wurde, stellt die Option sicher, dass jedes Mal, wenn sich Quest One ActiveRoles-Berechtigungszuteilungen oder -vorlagen ändern, sich auch die entsprechenden systemeigenen Berechtigungseinträge entsprechen ändern.

ADSI-Provider und Skriptrichtlinie zur Unterstützung der Anpassung

Quest One ActiveRoles bietet die Möglichkeit, die gebrauchsfertige Funktionalität mit Hilfe von Skripts und Anwendungen anzupassen, die mit dem Verwaltungsdienst in Zusammenhang stehen. ActiveRoles Server ermöglicht ein hohes Maß an benutzerdefinierten Änderungen, um den speziellen geschäftlichen und unternehmerischen Anforderungen zu entsprechen. Dies verleiht den Kunden eine höhere Flexibilität bei der Verwendung des Produkts und ermöglicht ihnen, Lösungen zu entwickeln, die ganz einfach in vorhandene Systeme und Daten integriert werden können. Die folgende Liste zeigt einige der Möglichkeiten, wie das Produkt angepasst werden kann:

- Mit Hilfe des Quest One ActiveRoles ADSI Provider könnten die vorhandenen Proprietär-Anwendungen oder benutzerdefinierten Web-basierten Schnittstellen mit Quest One ActiveRoles kommunizieren, um Verwaltungs- und Bereitstellungsaufgaben für Benutzerkonten und Gruppen auszuführen.
- Mit Hilfe von Richtlinienskripts können benutzerdefinierte Unternehmensregeln erzwungen werden, um Datenformate und administrative Arbeitsabläufe zu regeln.
- Mit Hilfe von Richtlinienskripts können die in einer HR-Datenbank oder in einem ERP-System gespeicherten Daten in die Verwaltung und Bereitstellung von Benutzern integriert werden.

Quest One ActiveRoles macht es vom Benutzer entwickelten Skripts und Anwendungen möglich, Directory-Objekte durch den Verwaltungsdienst (*beständige Objekte*) zu bearbeiten und die Kontrolle über Objekte zu erlangen, die gerade mit Quest One ActiveRoles (*In-Process-Objekten*) erstellt, geändert oder gelöscht werden.

Programmtechnischen Zugriff auf beständige und In-Process-Objekte zu haben macht es Entwicklern einfach, Quest One ActiveRoles in diesen beiden Bereichen anzupassen:

- Erstellen von benutzerdefinierten Anwendungen und Benutzerschnittstellen
- Erzwingen von administrativen Unternehmensrichtlinien durch Ausführung von benutzerdefinierten Skripts (*Skriptrichtlinien*)

Benutzerdefinierte Anwendungen und Benutzerschnittstellen

Eine benutzerdefinierte Anwendung oder Benutzerschnittstelle kann erstellt werden, um Directory-Objekte in Quest One ActiveRoles zu bearbeiten. Quest One ActiveRoles bietet den ADSI Provider, um mit Hilfe von Standard-COM-Schnittstellen, die die Microsoft ADSI 2.5-Spezifikation erfüllen, mit dem Verwaltungsdienst zu kommunizieren.

Benutzerdefinierte Anwendungen sind ausführbare Dateien, die Daten für den Verwaltungsdienst bereitstellen oder Daten vom Verwaltungsdienst abrufen und verarbeiten. So kann zum Beispiel eine Organisation mit einer Humanressourcen-Datenbank eine benutzerdefinierte Anwendung entwickeln und bereitstellen, die persönliche Informationen aus der Datenbank extrahiert und dann an den Verwaltungsdienst weiterleitet, um die Bereitstellung von Benutzerkonten zu erleichtern.

Benutzerdefinierte Benutzerschnittstellen sind normalerweise webbasierte Schnittstellen, die bestimmte Aufgaben an die Benutzer übertragen. Benutzerdefinierte Benutzerschnittstellen können auch verwendet werden, um den Arbeitsablauf von Netzwerkadministratoren und Help Desk-Mitarbeitern zu rationalisieren. So können zum Beispiel webbasierte Seiten erstellt werden, sodass Help Desk-Mitarbeitern nur die Felder angezeigt werden, die mit Benutzereigenschaften in Verbindung stehen, die sie gemäß den Unternehmensstandards anzeigen und ändern können.

Die benutzerdefinierten Anwendungen und Benutzerschnittstellen beruhen auf dem Quest One ActiveRoles ADSI Provider, um Zugriff auf die Funktionalität von Quest One ActiveRoles zu erlangen.

Benutzerdefinierte Skriptrichtlinien

Quest One ActiveRoles bietet die Möglichkeit, Verwaltungsrichtlinien durch Ausführung von von Benutzern entwickelten Skripts zu implementieren. Dies ermöglicht folgende Aktionen:

- **Erleichtern der Bereitstellung von Benutzerkonten.** Füllen der Benutzereigenschaften durch Integration einer externen Datenbank und Automatisierung von aus mehreren Schritten bestehenden Bereitstellungsaufgaben.
- **Wahrung der Integrität von Verzeichnisinhalten.** Verhindern von Inkonsistenzen zwischen Active Directory-Daten durch Erzwingen von Aktualisierungssequenz- und Datenformatrichtlinien im gesamten Unternehmen.
- **Erzwingen von Business-Regeln.** Wahrung des Sicherheitskonzepts und Sammeln von Verwaltungserfahrungen durch die Integration von Business-Regeln in den administrativen Arbeitsablauf.

Nach erfolgreicher Konfiguration werden die benutzerdefinierten, skriptbasierten Richtlinien ohne Interaktion mit dem Benutzer erzwungen. Quest One ActiveRoles führt automatisch die Richtlinienskripts aus, die besondere administrative Vorgänge erweitern und zusätzliche Verwaltungsvorgänge auslösen. Richtlinienskripts können zum Beispiel für folgende Aktionen verwendet werden:

- Durchführen einer hoch entwickelten Gültigkeitsprüfung für Eingangsdaten
- Synchrone Änderung von Informationen in mehreren Datenquellen wie etwa dem Active Directory-Speicher, dem Microsoft Exchange-Server und den Datenbanken des HR- oder ERP-Systems
- Sicherstellen, dass die delegierten Administratoren einen vorgegebenen administrativen Arbeitsablauf einhalten
- Verknüpfen von mehreren Verwaltungsaufgaben in einer Operatortransaktion

Dynamische Gruppen

Quest One ActiveRoles hilft die Gruppenverwaltung durch dynamische Festlegung der Gruppenzugehörigkeit anhand rollenbasierter Zugehörigkeitskriterien zu beschleunigen. Die dynamische Gruppenmitgliedschaft verhindert die Notwendigkeit zur manuellen Aktualisierung von Mitgliedschaftslisten für Sicherheits- und Verteilergruppen.

Zur Automatisierung der Pflege der Mitgliederverzeichnisse der Gruppen bietet Quest One ActiveRoles folgende Funktionen:

- Regelbasierter Mechanismus, der immer dann, wenn die Objektattribute in Active Directory geändert werden, automatisch Objekte zu Gruppen hinzufügt und entfernt
- Flexible Mitgliedschaftskriterien, die sowohl das abfragebasierte als auch das statische Füllen von Gruppen ermöglichen.

Die Mitgliedschaftskriterien fallen in die folgenden Kategorien:

- **Explizit einschließen.** Gewährleistet, dass die angegebenen Objekte unabhängig von jeglichen an den Objekten vorgenommenen Änderungen in der Mitgliedschaftsliste enthalten sind.
- **Nach Abfrage einschließen.** Füllt die Mitgliedschaftsliste mit Objekten, die bestimmte Eigenschaften aufweisen. Wenn ein Objekt erstellt wird, oder wenn sich seine Eigenschaften ändern, fügt es Quest One ActiveRoles in der Mitgliedschaftsliste hinzu oder entfernt es, je nachdem, ob die Objekteigenschaften die Suchkriterien erfüllen oder nicht.
- **Gruppenmitglieder einschließen.** Füllt die Mitgliedschaftsliste mit Mitgliedern von bestimmten ausgewählten Gruppen. Wenn ein Objekt in den gewählten Gruppen hinzugefügt oder entfernt wird, fügt Quest One ActiveRoles dieses Objekt in der Mitgliedschaftsliste hinzu oder entfernt es.
- **Explizit ausschließen.** Gewährleistet, dass die angegebenen Objekte unabhängig von jeglichen an den Objekten vorgenommenen Änderungen nicht in der Mitgliedschaftsliste enthalten sind.
- **Durch Abfrage ausschließen.** Stellt sicher, dass Objekte mit bestimmten Eigenschaften sich nicht in der Mitgliedschaftsliste befinden. Quest One ActiveRoles entfernt automatisch die Objekte aus der Mitgliedschaftsliste, je nachdem, ob die Objekteigenschaften die Suchkriterien erfüllen.
- **Gruppenmitglieder ausschließen.** Gewährleistet, dass Mitglieder der angegebenen Gruppen nicht in der Mitgliedschaftsliste enthalten sind. Wenn ein Objekt in einer der gewählten Gruppen hinzugefügt wird, wird Quest One ActiveRoles dieses Objekt automatisch aus der Mitgliedschaftsliste entfernt.

Diese Mitgliedschaftskriterien gelten auch für verwaltete Einheiten.

Betrieb in Umgebungen mit mehreren Gesamtstrukturen

Active Directory organisiert Netzwerkelemente in einer hierarchischen Struktur auf der Grundlage des Konzepts der Container, wobei der Container der obersten Ebene als eine Gesamtstruktur bezeichnet wird. Heutzutage bestehen zahlreiche Active Directory-Implementierungen aus mehreren Gesamtstrukturen. Die üblichen Gründe für das Vorhandensein von Implementierungen mehrerer Gesamtstrukturen sind die Isolation der administrativen Verwaltungsstellen, Fragen der Organisationsstruktur (z.B. autonome Unternehmenseinheiten und dezentralisierte IT-Abteilungen), die Unternehmensstrategie oder gesetzliche oder behördliche Anforderungen.

Dieser Abschnitt erteilt Informationen über die Funktionen und Vorteile von Quest One ActiveRoles bei Anwendung auf Umgebungen, wo mehrere Active-Directory-Gesamtstrukturen bereit gestellt wurden.

Mit Quest One ActiveRoles kann man eine skalierbare, sichere und verwaltbare Infrastruktur erstellen, die das Benutzer- und Ressourcen-Management in einer Umgebung mit mehreren Gesamtstrukturen vereinfacht. Vorteile der Bereitstellung von Quest One ActiveRoles in solchen Umgebungen:

- Zentralisierte Verwaltung von Verzeichnisdaten in Domänen, die zu verschiedenen Gesamtstrukturen gehören
- Administrative Ansichten, die die Grenzen der Gesamtstruktur überschreiten

- Möglichkeit zum Delegieren der administrativen Kontrolle über Verzeichnisdaten, wo dies angebracht ist, ohne Berücksichtigung der Grenzen der Gesamtstruktur
- Richtlinienbasierte Kontrolle und Automatisierung der Verwaltung der Verzeichnisdaten über die Grenzen von Gesamtstrukturen hinweg

Durch Registrierung der Active-Directory-Domänen in Quest One ActiveRoles bildet man eine Sammlung verwalteter Domänen, die eine Quest One ActiveRoles Sicherheits- und Verwaltungsbegrenzung in Active Directory darstellen. Die Zusammenstellung muss nicht auf Domänen aus einer einzigen Gesamtstruktur beschränkt sein. Stattdessen kann man Domänen aus jeder beliebigen Gesamtstruktur in seiner Umgebung registrieren, indem man den Quest One ActiveRoles-Verwaltungsdienst konfiguriert, um die entsprechenden administrativen Anmeldeinformationen pro Domäne zu verwenden.

Um die Verwaltung der Directory-Daten durch die verwalteten Domänen zu zentralisieren, ruft Quest One ActiveRoles die Active-Directory-Schemadefinitionen aus allen Gesamtstrukturen, zu welchen diese Domänen gehören, ab und konsolidiert sie. Die konsolidierte Schemabeschreibung wird in der Quest One ActiveRoles Konfigurationsdatenbank gespeichert und enthält Informationen über die Objektklassen und die Attribute der Objektklassen, die in den verwalteten Domänen gespeichert werden können. Durch Verwendung des konsolidierten Schemas erweitert Quest One ActiveRoles den Umfang seiner administrativen Vorgänge, um die gesamte Sammlung verwalteter Domänen ohne Berücksichtigung von Gesamtstrukturbeschränkungen abzudecken.

Quest One ActiveRoles ermöglicht es Administratoren, Directory-Objekte (wie Benutzer, Gruppen, Rechner usw.) innerhalb einer relationalen Struktur aus rollenbasierten administrativen Ansichten (genannt Verwaltungseinheiten) zu organisieren, von welchen jede nur diejenigen Objekte beinhaltet, die bestimmte, vom Administrator festgelegte Zugehörigkeitskriterien erfüllen. Diese Struktur kann unabhängig von logischen Modell von Active Directory erstellt werden, das auf dem Konzept der Container beruht und somit starre Grenzen zwischen Containern impliziert, ganz gleich, ob es sich dabei um Gesamtstrukturen, Domänen oder Organisationseinheiten handelt. Administratoren können verwaltete Einheiten so konfigurieren, dass jede Einheit die entsprechende Zusammenstellung von Verzeichnisobjekten repräsentiert, die im selben Active Directory-Container oder in verschiedenen Containern vorhanden sind, wobei verschiedene Gesamtstrukturen nicht die Ausnahme sind.

Um die Verwaltung der Directory-Daten zu vereinfachen, sorgt Quest One ActiveRoles für die administrative Delegierung sowohl auf der Ebene der verwalteten Einheit als auch auf der Ebene der individuellen Container in Active Directory. Durch die Delegation kann die Autorität über Verzeichnisobjekte, die sich in einer bestimmten Einheit oder in einem bestimmten Container befinden, an gewisse Benutzer oder Gruppen übertragen werden. Die Delegation der Kontrolle über verwaltete Einheiten bietet die Möglichkeit, die Verwaltung von Verzeichnisdaten auf Einzelpersonen aufzuteilen, denen zugetraut wird, die Verwaltung von bestimmten Gruppen und Objekttypen durchzuführen, ohne die Position der Objekte in der Active Directory-Struktur zu berücksichtigen. Dadurch macht es Quest One ActiveRoles einfach, die Kontrolle über die Directory-Daten aus einer Gesamtstruktur an Benutzer oder Gruppen zu delegieren, die sich in der gleichen oder einer anderen Gesamtstruktur befinden.

Quest One ActiveRoles ermöglicht auch die Implementierung der richtlinienbasierten Kontrolle und Automatisierung des Directory-Datenmanagements auf der Ebene der verwaltete Einheit. Durch die Anwendung von Richtlinien und Automatisierungsregeln auf verwaltete Einheiten können Administratoren eine konsistente Kontrolle einer genau definierten Zusammenstellung von Verzeichnisobjekten, die sich in verschiedenen Organisationseinheiten, Domänen oder Gesamtstrukturen befinden, gewährleisten. Darüber hinaus können Richtlinien und Automatisierungsregeln einheitlich auf verschiedene Container – ob in derselben Gesamtstruktur oder in verschiedenen Gesamtstrukturen – angewandt werden, was eine Plattform für komplexe Automatisierungsszenarien bietet, die auch gesamtstrukturübergreifende Vorgänge umfassen können. Ein Beispiel ist die Bereitstellung von Ressourcen einer Gesamtstruktur für die Benutzer einer anderen Gesamtstruktur.

Durch Hinzufügung von Objekten in einer Gruppe ermöglicht Quest One ActiveRoles Ihnen, Objekte aus unterschiedlichen verwalteten Domänen auszuwählen, einschließlich aus solchen, die zu anderen Gesamtstrukturen gehören. Dieser Vorgang erfordert eine Vertrauensstellung zwischen der Domäne, in der sich die Gruppe befindet, und der Domäne, in der sich das Objekt befindet, das Sie zur Gruppe hinzufügen möchten. Ansonsten verweigert Active Directory den Vorgang und erlaubt Ihnen Quest One ActiveRoles deshalb nicht, das Objekt zu wählen. Beachten Sie, dass Active Directory automatisch Vertrauensstellungen zwischen Domänen innerhalb einer Gesamtstruktur erstellt. Für Domänen in unterschiedlichen Gesamtstrukturen müssen Administratoren explizit Vertrauensstellungen definieren.

Die rollenbasierten Mechanismen, die Quest One ActiveRoles zur Verfügung stellt, um die Gruppen automatisch aufzufüllen, können auch in Umgebungen mit mehreren Gesamtstrukturen frei verwendet werden. Sie können Regeln konfigurieren, damit Quest One ActiveRoles Gruppen mit Objekten auffüllt, die sich in unterschiedlichen Domänen befinden, entweder in der gleichen Gesamtstruktur oder in anderen Gesamtstrukturen. Jedoch werden die Fähigkeiten von Quest One ActiveRoles, Gruppenzugehörigkeitslisten automatisch zu verwalten, auch durch Active-Directory-Einschränkungen eingeschränkt, die nur einer Gruppe erlauben, Objekte aus der Domäne zu beinhalten, zu welcher die Gruppe gehört, oder aus Domänen, denen diese Domäne vertraut. In anderen Wort ausgedrückt heißt das, dass, wenn kein Vertrauensverhältnis zwischen der Domäne besteht, zu welcher die Gruppe gehört, und der Domäne, zu welcher ein bestimmtes Objekt gehört, kann das Objekt weder manuell noch automatisch von Quest One ActiveRoles in die Gruppe eingefügt werden.

2

Erste Schritte

- Starten der Quest One ActiveRoles-Konsole
- Überblick über die Benutzerschnittstelle
- Anzeigemodus
- Verwenden verwalteter Einheiten
- Einrichten eines Filters
- Suchen nach Objekten
- Abrufen richtlinienbezogener Informationen

Starten der Quest One ActiveRoles-Konsole

Die Quest One ActiveRoles-Konsole, auch als MMC-Schnittstelle bezeichnet, ist ein umfassendes Verwaltungstool für Active Directory und Microsoft Exchange. Mit der Quest One ActiveRoles-Konsole können Sie ganz einfach Verzeichnisobjekte finden und administrative Aufgaben ausführen.

Aufrufen der Programmsteuerung von Quest One ActiveRoles

- Wählen Sie **Start | Alle Programme | Quest-Software | Quest One ActiveRoles**, und klicken Sie auf **Quest One ActiveRoles-Konsole**.

In der Regel wählt die Quest One ActiveRoles-Konsole automatisch den Administrationsdienst und stellt eine Verbindung her. Kann die Konsole keine Verbindung zum Administrationsdienst herstellen, oder möchten Sie den Administrationsdienst manuell auswählen, siehe den Abschnitt „Verbinden mit dem Administrationsdienst" im *Quest One ActiveRoles-Administratorhandbuch*.

Erhalten und Verwenden der Hilfe

Die Quest One ActiveRoles-Hilfe erläutert Konzepte und umfasst Anweisungen zum Ausführen von Aufgaben mit dem Produkt.

Sie können die folgenden Richtlinien verwenden, um bei der Arbeit Unterstützung zu erhalten:

- Klicken Sie für den Zugriff auf die Quest One ActiveRoles-Hilfe auf **Hilfe** im Menü **Aktion** oder auf **Hilfethemen** im Menü **Hilfe**.
- Klicken Sie zum Anzeigen der Beschreibung eines Dialogfelds auf die Schaltfläche **Hilfe** im Dialogfeld, oder drücken Sie die Taste F1.
- Wenn Sie eine kurze Beschreibung eines Menübefehls oder einer Schaltfläche in der Symbolleiste anzeigen möchten, zeigen Sie auf den Befehl oder die Schaltfläche. Die Beschreibung wird in der Statuszeile am unteren Fensterrand angezeigt.

Sie können ein Hilfethema oder alle Hilfethemen unter der ausgewählten Überschrift anzeigen.

So drucken Sie ein einzelnes Hilfethema:

1. Klicken Sie in der Menüleiste auf **Hilfe** und dann auf **Hilfethemen**.
2. Erweitern Sie im linken Bereich der Hilfeanzeige die Überschrift mit dem gewünschten Hilfethema. Klicken Sie dann auf das Thema.
3. Klicken Sie in der Symbolleiste der Hilfeanzeige auf **Optionen** und dann auf **Drucken**.
4. Klicken Sie auf **OK**, um nur das gewählte Thema zu drucken.

So drucken Sie alle Hilfethemen unter einer Überschrift:

1. Klicken Sie in der Menüleiste auf **Hilfe** und dann auf **Hilfethemen**.
2. Klicken Sie im linken Bereich der Hilfeanzeige auf die Überschrift mit dem gewünschten Hilfethema.
3. Klicken Sie in der Symbolleiste der Hilfeanzeige auf **Optionen** und dann auf **Drucken**.
4. Klicken Sie im Dialogfeld **Themen drucken** auf **Ausgewählte Überschrift und alle Unterthemen drucken**, und klicken Sie auf **OK**.

Überblick über die Benutzerschnittstelle

Das Quest One ActiveRoles-Konsolenfenster ist in zwei Bereiche unterteilt. Der linke Bereich enthält den Konsolenbaum mit den in der Konsole verfügbaren Elementen. Der rechte Bereich (Detailbereich) enthält Informationen zu den Elementen, die im Konsolenbaum ausgewählt werden. Sie können die meisten Management-Aufgaben von diesem Bereich aus mit Befehlen aus dem Menü **Aktion** durchführen.

Weitere Informationen werden im unteren Teilbereich des Detailfensters angezeigt, wenn Sie den Befehl **Erweiterter Detailbereich** im Menü **Anzeigen** auswählen. Sie können Management-Aufgaben aus dem unteren Teilbereich mit Befehlen aus dem Menü **Aktion** durchführen.

Konsolenstruktur

Der linke Bereich der Quest One ActiveRoles-Konsole enthält den Konsolenbaum.

Der Stamm des Konsolenbaums ist mit **Quest One ActiveRoles** gekennzeichnet. Der Name des Administrationsdiensts wird in eckigen Klammern angegeben. Haben Sie den erweiterten Anzeigemodus für die Quest One ActiveRoles-Konsolenanzeige ausgewählt (**Anzeigen | Modus**), werden die folgenden Ordner unter dem Stamm des Konsolenbaums angezeigt:

- **Konfiguration.** Enthält alle proprietären Quest One ActiveRoles-Objekte in Containern mit entsprechenden Namen.
- **Active Directory.** Enthält eine Liste der Domains, die in Quest One ActiveRoles registriert sind. In diesem Ordner können Sie Domänen nach Verzeichnisobjekten (Benutzer, Gruppen, Computer) durchsuchen und Verwaltungsaufgaben für diese Objekte ausführen.
- **AD LDS (ADAM).** Enthält eine Liste der AD LDS-Verzeichnispartitionen, die in Quest One ActiveRoles registriert sind. In diesem Ordner können Sie Partitionen nach Verzeichnisobjekten (Benutzer, Gruppen, Container) durchsuchen und Verwaltungsaufgaben für diese Objekte ausführen.
- **Anwendungen.** Enthält eine Liste der Anwendungen, die mit Quest One ActiveRoles integriert wurden (z. B. Reporting). Ermöglicht den schnellen Zugriff auf diese Anwendungen.

Der Konsolen-Anzeigemodus legt fest, welche Ordner im Konsolenbaum angezeigt werden. Weitere Informationen finden Sie unter „Anzeigemodus" weiter hinten in diesem Dokument.

Bereich „Details"

Wenn Sie ein Element im Konsolenbaum auswählen, ändert sich der Detailbereich entsprechend. Wenn Sie administrative Aufgaben ausführen möchten, klicken Sie im Detailbereich auf Elemente, und verwenden Sie die Befehle im Menü **Aktion**. Die Befehle im Menü **Aktion** erscheinen auch im Schnellzugriffsmenü, dass Sie durch Klicken mit der rechten Maustaste auf Elemente im Konsolenbaum oder im Detailbereich aufrufen können.

Standardmäßig werden die Objekte im Detailbereich nach Objektname aufsteigend sortiert. Sie können die Sortierreihenfolge ändern, indem Sie auf eine Spaltenüberschrift klicken. Sie können Spalten im Detailbereich hinzufügen oder entfernen, indem Sie den Befehl **Spalten auswählen** im Menü **Anzeige** verwenden.

In der Quest One ActiveRoles-Konsole können Sie Filter auf den Detailbereich anwenden, um nach Verzeichnisobjekten zu suchen. Wenn Sie einen Filter konfigurieren möchten, wählen Sie eine Domäne, und klicken Sie auf **Filteroptionen** im Menü **Anzeige**. Sie können auch im Detailbereich nach einem Objekt suchen, indem Sie einige Zeichen eingeben. Auf diese Weise wird das erste Element in der sortierten Spalte gewählt, das den eingegebenen Zeichen entspricht.

Erweiterter Bereich

Der erweiterte Bereich erscheint am unteren Rand des Detailbereichs, wenn Sie die Option **Erweiterter Detailbereich** im Menü **Anzeigen** auswählen. Mit dem erweiterten Bereich können Sie ein Objekt verwalten, das Sie im Konsolenbaum oder im Detailbereich ausgewählt haben: Klicken Sie mit der rechten Maustaste auf einen vorhandenen Eintrag in der Liste, um diesen zu verwalten. Sie können auch mit der rechten Maustaste auf eine leere Stelle des erweiterten Bereichs klicken, um einen neuen Eintrag hinzuzufügen.

Der erweiterte Bereich besteht aus einer Reihe von Seiten mit Registerkarten. Das ausgewählte Objekt legt fest, welche Registerkarten angezeigt werden. Alle möglichen Registerkarten im erweiterten Bereich und deren Beschreibungen lauten wie folgt:

- **ActiveRoles-Sicherheit.** Zeigt Quest One ActiveRoles Zugriffsvorlagen für das ausgewählte Objekt
- **Links.** Zeigt die Objekte, auf die die ausgewählte Zugriffsvorlage angewendet wird
- **ActiveRoles-Richtlinie.** Zeigt Quest One ActiveRoles-Richtlinienvorlagen, die auf das ausgewählte Objekt angewendet werden
- **Native Sicherheit.** Listet Active Directory-Berechtigungseinträge für das ausgewählte Objekt auf
- **Mitglied von.** Listet Gruppen auf, zu denen das gewählte Objekt gehört
- **Mitglieder.** Listet Mitglieder der gewählten Gruppe auf

Die Konsole zeigt die Registerkarten **ActiveRoles-Sicherheit**, **ActiveRoles-Richtlinie** und **Native Sicherheit** nur dann für ein ausgewähltes Objekt, wenn Ihr Benutzerkonto das Recht **Lesekontrolle** für das gewählte Objekt enthält.

Je nach der im erweiterten Bereich gewählten Registerkarte zeigt die Symbolleiste die folgenden Schaltflächen, um Sie bei der Arbeit mit den Einträgen auf der Registerkarte zu unterstützen.

ActiveRoles-Sicherheit, Links

	Anwenden weiterer Zugriffsvorlagen auf das gewählte Objekt
	Anzeigen von Zugriffsvorlagen, die das gewählte Objekt aufgrund von Vererbung betreffen
	Synchronisieren von Quest One ActiveRoles-Sicherheit mit Active Directory-Sicherheit

ActiveRoles-Richtlinie

	Anwenden weiterer Richtlinienobjekte auf das gewählte Objekt
	Anzeigen von Richtlinienobjekten, die das gewählte Objekt aufgrund von Vererbung betreffen

Einheitliche Sicherheit

	Anzeigen von Berechtigungseinträgen, die von übergeordneten Objekten übernommen werden
	Anzeigen von Standard-Berechtigungseinträgen, die nach dem AD-Schema angegeben werden

Mitglied von, Mitglieder

	Hinzufügen des gewählten Objekts zu Gruppen
	Definieren der Gruppe als primäre Gruppe für das gewählte Objekt

Anzeigemodus

In der Quest One ActiveRoles-Konsole können Sie den Anzeigemodus Basis, Erweitert oder Unformatiert wählen. Die Änderung des Ansichtsmodus ermöglicht Ihnen, erweiterte Objekte und Container aus der Anzeige herauszufiltern.

Das Basismodus zeigt Active Directory-Objekte und verwaltete Einheiten und filtert Objekte bzw. Container je nach Quest One ActiveRoles-Konfiguration heraus. Der Standardmodus sollte normalerweise von delegierten Administratoren und Help Desk-Mitarbeitern verwendet werden.

Der erweiterte Modus zeigt alle Objekte und Container mit Ausnahme der für die interne Nutzung in Quest One ActiveRoles reservierten an. Der erweiterte Modus ist für Administratoren konzipiert, die für die Konfiguration des Systems und für die Verwaltung von proprietären Quest One ActiveRoles-Objekten verantwortlich sind.

Der unformatierte Modus zeigt alle Objekte und Container im Quest One ActiveRoles-Namespace an. Dieser Modus wird primär für Problembehandlungszwecke verwendet.

Im unformatierten Modus zeigt die Konsole alle Daten an, die vom Administrationsdienst abgerufen werden. Im Basis- oder erweiterten Modus werden einige Daten herausgefiltert. Der Ordner **Konfiguration** wird z. B. im Basismodus nicht im Konsolenbaum angezeigt. Ein weiteres Beispiel ist der Ordner **Konfigurationscontainer** zur Anzeige des Active Directory-Konfigurations-Benennungskontexts. Dieser wird nur im unformatierten Modus angezeigt. Außerdem gibt es einige Befehle und Eigenschaftenseiten, die nur dann angezeigt werden, wenn sich die Konsole im unformatierten Modus befindet.

Kurz gesagt: Wenn Sie den unformatierten Modus verwenden, werden alle Daten angezeigt, die angezeigt werden können. Andernfalls werden einige Elemente ausgeblendet. Beachten Sie, dass durch Ändern des Ansichtsmodus keine Elemente verändert werden. Damit werden nur Elemente ein- oder ausgeblendet.

Klicken Sie zum Ändern des Ansichtsmodus auf **Modus** im Menü **Anzeige**. Klicken Sie im Dialogfeld **Anzeigemodus** auf **Basismodus**, **Erweiterter Modus** oder **Unformatierter Modus**.

Kontrollierte Objekte

Die Quest One ActiveRoles-Konsole bietet eine visuelle Darstellung der Objekte, mit denen Zugriffsvorlagen oder Richtlinienobjekte verbunden werden. Die Konsole markiert diese Objekte durch Hinzufügen eines Pfeilsymbols an der unteren linken Ecke des Symbols, das das Objekt in der Konsolenstruktur oder im Detailfenster repräsentiert. Daher sieht das Symbol wie in der folgenden Abbildung aus:

Wenn Sie diese Funktion aktivieren möchten, klicken Sie auf **Kontrollierte Objekte markieren** im Menü **Anzeige**, und wählen Sie die Optionen zur Definition der zu markierenden Objektkategorie aus.

Verwenden verwalteter Einheiten

Quest One ActiveRoles umfasst diese Sicherheits- und Verwaltungselemente:

- **Trustees.** Benutzer oder Gruppen, die über die Berechtigungen zur Verwaltung von Benutzern, Gruppen, Computern oder anderen Verzeichnisobjekten verfügen.
- **Berechtigungen und Rollen.** Berechtigungen sind in Zugriffsvorlagen (Rollen) gruppiert, die definieren, wie ein Trustee Verzeichnisobjekte verwalten kann.
- **Verwaltete Einheiten.** Auflistungen von Verzeichnisobjekten, die für die Verwaltung an Trustees delegiert werden.

Der Verzeichnisadministrator legt fest, welche Benutzer oder Gruppen Trustees sind, welche Rollen und Berechtigungen den Trustees zugewiesen sind und welche Objekte in den verwalteten Einheiten enthalten sind.

Mit verwalteten Einheiten wird bestimmt, welche Verzeichnisobjekte ein Trustee verwalten kann. Als Trustee können Sie die verwalteten Einheiten administrieren, für die Ihnen Berechtigungen zugewiesen sind. Verwaltete Einheiten, die Objekte enthalten, die Sie verwalten dürfen, werden in der Konsolenstruktur unter **Verwaltete Einheiten** angezeigt.

Wenn Sie eine verwaltete Einheit in der Konsolenstruktur auswählen, zeigt der Bereich „Details" eine Liste der in dieser verwalteten Einheit enthaltenen Objekte an. Um Objekte zu verwalten, wählen Sie sie in der Liste aus und verwenden Sie die Befehle im Menü **Aktion**.

Wenn eine verwaltete Einheit einen Container wie etwa eine Organisationseinheit enthält, dann wird der Container in der Konsolenstruktur unter „Verwaltete Einheit", wie in der Abbildung dargestellt, angezeigt. Wenn Sie einen Container in der Konsolenstruktur auswählen, werden im Bereich „Details" alle in diesem Container enthaltenen untergeordneten Objekte und Untercontainer aufgelistet.

Einrichten eines Filters

Quest One ActiveRoles-Konsole ermöglicht die Anwendung eines Filters, um nur die Objekte anzuzeigen, die den Filterkriterien entsprechen. Um einen Filter anzuwenden, wählen Sie ein Active Directory-Objekt oder einen Container aus und klicken Sie dann auf die Schaltfläche **Filter** in der Symbolleiste: Hierdurch wird das Dialogfeld **Filteroptionen** angezeigt, in dem Sie einen Filter einrichten können. Nachdem Sie den Filter festgelegt haben, werden die Filterkriterien sofort auf alle Active Directory-Objektlisten in der Quest One ActiveRoles-Konsole angewandt.

Schritte zum Sortieren und Filtern von Listen im Detailfenster

So sortieren Sie Objekte im Bereich „Details"

1. Klicken Sie auf eine Spaltenüberschrift, um die Tabelle nach den Inhalten dieser Spalte zu sortieren.
2. Klicken Sie erneut auf die Spaltenüberschrift, um zwischen der aufsteigenden und absteigenden Sortierreihenfolge zu wechseln.

Gehen Sie folgendermaßen vor, um Spalten zum Bereich „Details" hinzuzufügen bzw. aus ihm zu entfernen

1. Klicken Sie im Menü **Ansicht** auf **Spalten auswählen** oder **Spalten hinzufügen/ entfernen**.
2. Gehen Sie folgendermaßen vor und klicken Sie dann auf **OK**:
   - Um eine Spalte hinzuzufügen, klicken Sie unter **Verfügbare Spalten** auf die Spalte, die Sie anzeigen möchten, und klicken Sie dann auf **Hinzufügen**.
   - Um eine Spalte zu entfernen, klicken Sie unter **Angezeigte Spalten** auf die Spalte, die Sie ausblenden möchten, und klicken Sie dann auf **Entfernen**.
   - Um die Spalten neu anzuordnen, klicken Sie auf einen Spaltennamen unter **Angezeigte Spalten** und klicken Sie dann auf **Nach oben** oder **Nach unten**, um die Position der Spalte zu ändern.

In der erweiterten Detailanzeige können Sie Spalten zu einer Liste im oberen oder unteren Teilbereich hinzufügen bzw. entfernen: Klicken Sie im Teilbereich auf die Liste, die Sie ändern möchten, und befolgen Sie dann das oben aufgeführte Verfahren.

Filteroptionen unterstützen Sie bei der Suche nach bestimmten Objekten im Bereich „Details". Sie können alle Objekte oder nur Objekte des ausgewählten Typs anzeigen, die Anzahl der Elemente konfigurieren, die für jeden Ordner angezeigt werden können, oder benutzerdefinierte Filter mit Hilfe der Objektattribute und LDAP-Abfragen erstellen.

So wählen Sie Anzeigefilteroptionen

1. Klicken Sie im Menü **Ansicht** auf **Filteroptionen**.
2. Führen Sie einen der nachfolgend aufgeführten Schritte durch und klicken Sie dann auf **OK**
   - Klicken Sie zur Anzeige aller Objekte auf **Alle Objekttypen anzeigen**. Bei Auswahl dieser Option wird der Filter deaktiviert.
   - Klicken Sie zur Anzeige von Objekten eines bestimmten Typs auf **Nur folgende Objekttypen anzeigen** und aktivieren Sie die Kontrollkästchen neben den Objekttypen, die angezeigt werden sollen.
   - Um Objekte anzuzeigen, die mit benutzerdefinierten Filterkriterien übereinstimmen, klicken Sie auf **Benutzerdefinierten Filter erstellen**. **Passen** Sie dann Ihre Filterkriterien an und konfigurieren Sie sie, indem Sie die unter Verfahren zum Anlegen einer benutzerdefinierten Suche aufgeführten Anweisungen befolgen.

3. Ändern Sie optional unter **Maximal pro Ordner angezeigte Elemente** die maximale Anzahl der Objekte, die in der Konsole angezeigt werden können. Der Standardwert für die maximale Anzahl der in der Konsole angezeigten Objekte lautet 2.000.

Suchen nach Objekten

Mit der Quest One ActiveRoles-Konsole können Sie mit Hilfe des Fensters **Suchen** nach Objekten verschiedenen Typs suchen. Um das Fenster **Suchen** aufzurufen, klicken Sie mit der rechten Maustaste auf einen Container und klicken Sie dann auf **Suchen**.

In der Liste **In** können Sie den zu suchenden Container oder die zu suchende verwaltete Einheit auswählen. Die Liste enthält den Container, den Sie vor dem Aufruf des Fensters **Suchen** ausgewählt haben. Klicken Sie auf **Durchsuchen**, um Container zur Liste hinzuzufügen. In der Liste **Suchen** können Sie den Objekttyp auswählen, den Sie suchen möchten.

Wenn Sie einen Objekttyp auswählen, wird das Fenster **Suchen** entsprechend geändert. Beispielsweise wird mit **Benutzer, Kontakte und Gruppen** nach Benutzern, Kontakten oder Gruppen gesucht, indem Kriterien, wie der Benutzername, eine beschreibende Notiz zu einem Kontakt oder der Name einer Gruppe, verwendet werden. In der Liste **Suchen** teilt Quest One ActiveRoles die Kategorie **Benutzer, Kontakte und Gruppen** in drei auf, um so eine rationalisierte Suche zu ermöglichen.

Durch Auswahl von **Benutzerdefinierte Suche** aus der Liste **Suchen** können Sie benutzerdefinierte Suchanfragen mit Hilfe der erweiterten Suchoptionen erstellen:

Im Fenster **Suchen** können Sie nach beliebigen Verzeichnisobjekten suchen, z. B. nach Benutzern, Gruppen, Computern, Organisationseinheiten, Druckern oder freigegebenen Ordnern. Sie können auch nach Konfigurationsobjekten von Quest One ActiveRoles suchen, z. B. nach Zugriffsvorlagen, verwalteten Einheiten und Richtlinienobjekten. Wenn Sie nach Zugriffsvorlagen, Richtlinienobjekten oder verwalteten Einheiten suchen und in der Liste **Suchen** einen entsprechenden Objekttyp auswählen, wird der jeweilige Container in der Liste **In** angezeigt.

Wenn die Suche abgeschlossen ist, werden die den Suchkriterien entsprechenden Objekte (die Suchergebnisse) unten im Fenster **Suchen** aufgelistet. Sie können auf schnelle Art ein Objekt in der Suchergebnisliste finden, indem Sie einige Zeichen eingeben. Hierdurch wird der erste Name ausgewählt, der mit den von Ihnen eingegebenen Zeichen übereinstimmt.

Wenn Sie das Objekt gefunden haben, können Sie es verwalten, indem Sie den Eintrag in der Suchergebnisliste mit der rechten Maustaste anklicken und dann auf die Befehle im Kontextmenü klicken.

Verfahren zum Suchen nach einem Benutzer, Kontakt oder einer Gruppe

So suchen Sie nach einem Benutzer, Kontakt oder einer Gruppe

1. Klicken Sie im Menü **Aktion** auf **Suchen**, um das Fenster **Suchen** anzuzeigen.
2. Klicken Sie im Feld **Suchen** auf eines der folgenden Elemente:
   - **Benutzer, Kontakte und Gruppen**, um alle Benutzer, Gruppen und Kontakte zu suchen, die mit Ihren Suchkriterien übereinstimmen.
   - **Benutzer**, um nur Benutzer zu suchen, die mit Ihren Suchkriterien übereinstimmen.
   - **Gruppen**, um nur Gruppen zu suchen, die mit Ihren Suchkriterien übereinstimmen.
   - **Kontakte**, um nur Kontakte zu suchen, die mit Ihren Suchkriterien übereinstimmen.

3. Wählen Sie im Feld **In** die Domäne, den Container oder die verwaltete Einheit aus, die bzw. den Sie suchen möchten, oder klicken Sie auf **Durchsuchen**, um eine Domäne, einen Container oder eine verwaltete Einheit zu suchen.
4. Geben Sie einen Namen, eine Beschreibung oder Beides ein:
   - Geben Sie in das Feld **Name** den Namen des gesuchten Objekts ein.
   - Geben Sie in das Feld **Beschreibung** die Beschreibung des gesuchten Objekts ein.

   *Sie können die Suche anhand teilweiser Suchkriterien durchführen. So gibt zum Beispiel **B** im Feld **Name** alle Objekte aus, deren Namen mit dem Buchstaben **B**, wie etwa „Backup-Operatoren", beginnen.*
5. Klicken Sie auf **Jetzt suchen**, um die Suche zu starten.

- Sie können die Registerkarte **Erweitert** verwenden, um erweiterte Suchoptionen anzugeben. Details finden Sie unter Verfahren zum Verwenden von erweiterten Optionen für die Suche.
- Die gefundenen Benutzer, Gruppen oder Kontakte werden unten im Fenster **Suchen** angezeigt.
- Sie können die gefundenen Benutzer, Gruppen oder Kontakte direkt ausgehend von der Liste im Fenster **Suchen** verwalten: Klicken Sie mit der rechten Maustaste auf ein Listenelement und verwenden Sie dann die Befehle im Kontextmenü, um Verwaltungsaufgaben durchzuführen.

Verfahren zum Suchen nach einem Computer

So suchen Sie nach einem Computer

1. Klicken Sie im Menü **Aktion** auf **Suchen**, um das Fenster **Suchen** anzuzeigen.
2. Klicken Sie im Feld **Suchen** auf **Computer**.
3. Wählen Sie im Feld **In** die Domäne, den Container oder die verwaltete Einheit aus, die bzw. den Sie suchen möchten, oder klicken Sie auf **Durchsuchen**, um eine Domäne, einen Container oder eine verwaltete Einheit zu suchen.
4. Geben Sie in das Feld **Name** den Namen des gesuchten Objekts ein.

   *Sie können die Suche anhand teilweiser Suchkriterien durchführen. So gibt zum Beispiel **B** im Feld **Name** alle Computer aus, deren Namen mit dem Buchstaben **B** beginnen.*
5. Klicken Sie optional im Feld **Rolle** auf eines der folgenden Elemente:
   - **Domänencontroller**, wenn Sie nur nach Domänencontrollern suchen möchten.
   - **Workstations und Server**, um nur nach Workstations und Servern (und nicht nach Domänencontrollern) zu suchen.
6. Klicken Sie auf **Jetzt suchen**, um die Suche zu starten.

- Sie können die Registerkarte **Erweitert** verwenden, um erweiterte Suchoptionen anzugeben. Details finden Sie unter Verfahren zum Verwenden von erweiterten Optionen für die Suche.
- Die gefundenen Computer werden unten im Fenster **Suchen** angezeigt.
- Sie können die gefundenen Computerobjekte direkt ausgehend von der Liste im Fenster **Suchen** verwalten: Klicken Sie mit der rechten Maustaste auf ein Listenelement und verwenden Sie dann die Befehle im Kontextmenü, um Verwaltungsaufgaben durchzuführen.

Verfahren zum Suchen nach einer Organisationseinheit

So suchen Sie nach einer Organisationseinheit

1. Klicken Sie im Menü **Aktion** auf **Suchen**, um das Fenster **Suchen** anzuzeigen.
2. Klicken Sie im Feld **Suchen** auf **Organisationseinheiten**.
3. Wählen Sie im Feld **In** die Domäne, den Container oder die verwaltete Einheit aus, die bzw. den Sie suchen möchten, oder klicken Sie auf **Durchsuchen**, um eine Domäne, einen Container oder eine verwaltete Einheit zu suchen.
4. Geben Sie in das Feld **Name** den Namen (oder einen Teil des Namens) der Organisationseinheit ein, die Sie suchen möchten.
5. Klicken Sie auf **Jetzt suchen**, um die Suche zu starten.

- Sie können die Registerkarte **Erweitert** verwenden, um erweiterte Suchoptionen anzugeben. Details finden Sie unter Verfahren zum Verwenden von erweiterten Optionen für die Suche.
- Die gefundenen Organisationseinheiten werden unten im Fenster **Suchen** angezeigt.
- Sie können die gefundenen Organisationseinheiten direkt ausgehend von der Liste im Fenster **Suchen** verwalten: Klicken Sie mit der rechten Maustaste auf ein Listenelement und verwenden Sie dann die Befehle im Kontextmenü, um Verwaltungsaufgaben durchzuführen.

Verfahren zum Verwenden von erweiterten Optionen für die Suche

So verwenden Sie erweiterte Optionen für die Suche

1. Klicken Sie im Menü **Aktion** auf **Suchen**, um das Fenster **Suchen** anzuzeigen.
2. Klicken Sie im Feld **Suchen** auf den Objekttyp, nach dem Sie suchen möchten.
3. Klicken Sie auf die Registerkarte **Erweitert**.
4. Klicken Sie auf die Schaltfläche **Feld** und wählen Sie die Objekteigenschaft aus, die Sie abfragen möchten.
5. Klicken Sie unter **Bedingung** auf die Bedingung für Ihre Suche und geben Sie dann unter **Wert** einen Eigenschaftswert ein, damit Ihre Suche die Objekte sucht, die die Objekteigenschaft haben, die mit dem von Ihnen angegebenen Bedingungswert-Paar übereinstimmen.
6. Klicken Sie auf **Hinzufügen**, um diese Suchbedingung zu Ihrer Suche hinzuzufügen.
7. Wiederholen Sie die Schritte 4 bis 6, bis Sie alle gewünschten Suchbedingungen hinzugefügt haben.
8. Klicken Sie auf eine der folgenden Optionen:
   - Wenn Sie die Objekte suchen möchten, die allen angegebenen Bedingungen entsprechen, klicken Sie auf **UND**.
   - Wenn Sie die Objekte suchen möchten, die einer beliebigen der angegebenen Bedingungen entsprechen, klicken Sie auf **ODER**.
9. Klicken Sie auf **Jetzt suchen**, um die Suche zu starten. Die gefundenen Objekte werden unten im Fenster angezeigt.

Verfahren zum Anlegen einer benutzerdefinierten Suche

So legen Sie eine benutzerdefinierte Suche an

1. Klicken Sie im Menü **Aktion** auf **Suchen**, um das Fenster **Suchen** anzuzeigen.
2. Klicken Sie im Feld **Suchen** auf **Benutzerdefinierte Suche**.
3. Wählen Sie im Feld **In** die Domäne, den Container oder die verwaltete Einheit aus, die bzw. den Sie suchen möchten, oder klicken Sie auf **Durchsuchen**, um eine Domäne, einen Container oder eine verwaltete Einheit zu suchen.

4. Führen Sie einen der nachfolgend aufgeführten Schritte aus:
   - Befolgen Sie auf der Registerkarte **Benutzerdefinierte Suche** die Schritte 4-9 des unter Verfahren zum Verwenden von erweiterten Optionen für die Suche beschriebenen Verfahrens.
   - Geben Sie auf der Registerkarte **Erweitert** einen Suchfilter mit Hilfe von LDAP-Syntax an.
5. Klicken Sie auf **Jetzt suchen**, um die Suche zu starten.

LDAP-Syntax

Mit Suchfiltern können Sie Suchkriterien definieren und effizientere und effektivere Suchvorgänge durchführen. Diese Suchfilter werden durch Unicode-Zeichenfolgen dargestellt.

Die Quest One ActiveRoles-Konsole unterstützt die standardmäßigen LDAP-Suchfilter, die in RFC2254 definiert sind.

In der folgenden Tabelle sind einige Beispiele für standardmäßige LDAP-Suchfilter aufgeführt.

SUCHFILTER	BESCHREIBUNG
`(objectClass=*)`	Alle Objekte
`(&(objectCategory=person)(objectClass=user)(!cn=andy))`	Alle Benutzerobjekte außer „andy“
`(sn=sm*)`	Alle Objekte, deren Nachname mit „sm“ beginnt
`(&(objectCategory=person)(objectClass=contact)(|(sn=Smith)(sn=Johnson)))`	Alle Kontakte mit dem Nachnamen „Smith“ oder „Johnson“

Suchfilter-Format

Suchfilter verwenden eines der folgenden Formate:

```
<filter>=(<attribute><operator><value>)

oder

<operator><filter1><filter2>)
```

In diesem Beispiel steht `<attribute>` für den LDAP-Anzeigenamen des Attributs, nach dem Sie suchen möchten.

Operatoren

In der folgenden Tabelle sind einige häufig verwendete Suchfilter-Operatoren aufgeführt.

LOGISCHER OPERATOR	BESCHREIBUNG
`=`	Ist gleich
`~=`	Entspricht in etwa
`<=`	Lexikografisch kleiner oder gleich
`>=`	Lexikografisch größer oder gleich
`&`	UND

LOGISCHER OPERATOR	BESCHREIBUNG
|	ODER
!	NICHT

Platzhalter

Bei Suchfiltern können Sie auch Platzhalter und Bedingungen verwenden. Die folgenden Beispiele enthalten Teilzeichenfolgen, mit denen nach dem Verzeichnis gesucht werden kann.

Alle Einträge abrufen:

```
(objectClass=*)
```

Einträge abrufen, die ’bob’ an einer beliebigen Stelle im allgemeinen Namen enthalten:

```
(cn=*bob*)
```

Einträge mit einem allgemeinen Namen abrufen, der größer als oder gleich ’bob’ ist:

```
(cn>=’bob’)
```

Alle Benutzer mit einem E-Mail-Attribut abrufen:

```
(&(objectClass=user)(mail=*))
```

Alle Benutzereinträge mit einem E-Mail-Attribut und dem Nachnamen gleich ’smith’ abrufen:

```
(&(sn=smith)(objectClass=user)(mail=*))
```

Alle Benutzereinträge mit einem allgemeinen Namen abrufen, der mit ’andy’, ’steve’ oder ’margaret’ anfängt:

```
(&(objectClass=user) | (cn=andy*)(cn=steve)(cn=margaret))
```

Alle Benutzer ohne E-Mail-Attribut abrufen:

```
(!(mail=*))
```

Sonderzeichen

Wenn eines der folgenden Sonderzeichen im Suchfilter als Literal verwendet wird, muss es durch die aufgeführte Escape-Sequenz ersetzt werden.

ASCII-ZEICHEN	ESCAPE-SEQUENZ-ERSATZ
*	\2a
(	\28
)	\29
\	\5c
NULL	\00

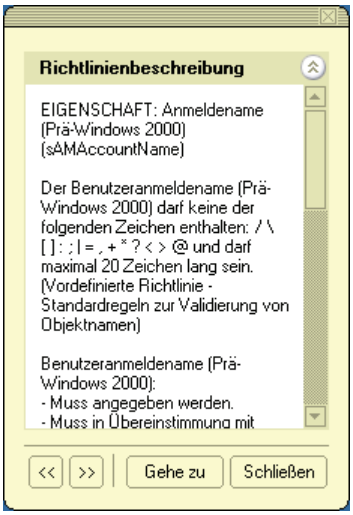
Außerdem können beliebige binäre Daten mit Hilfe der Escape-Sequenz-Syntax dargestellt werden, indem jedes Byte der binären Daten mit dem umgekehrten Schrägstrich (\) codiert wird, der von zwei hexadezimalen Zahlen gefolgt wird. Beispielsweise wird der Vier-Byte-Wert 0x00000004 in einer Filterzeichenfolge als \00\00\00\04 codiert.

Abrufen richtlinienbezogener Informationen

In Assistenten zur Objekterstellung und in Eigenschafts-Dialogfeldern können einige Eigenschaftsnamen als Hyperlinks angezeigt werden. Dies zeigt an, dass Quest One ActiveRoles Richtlinieneinschränkungen für die Eigenschaft durchsetzt.

In der folgenden Abbildung sind die Beschriftungen **Benutzeranmeldename** und **Benutzeranmeldename (Prä-Windows 2000)** unterstrichen. Dies bedeutet, dass diese Eigenschaften von einer bestimmten Richtlinie gesteuert werden, die mit Quest One ActiveRoles definiert wurde.

Um die Richtlinie eingehend zu überprüfen, können Sie auf deren Bezeichnung klicken. Wenn Sie beispielsweise auf **Benutzeranmeldename (Prä-Windows 2000)** klicken, zeigt die Quest One ActiveRoles-Konsole ein Fenster an, das dem in der folgenden Abbildung dargestellten Fenster entspricht.

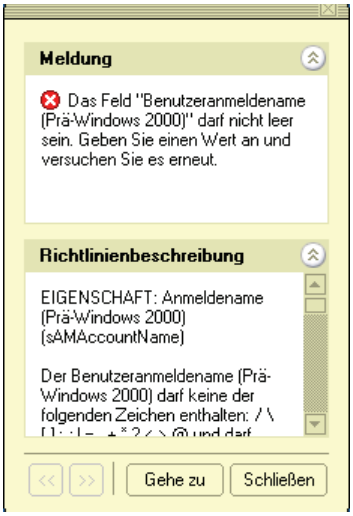

Richtlinienbeschreibung
EIGENSCHAFT: Anmeldename (Prä-Windows 2000) (sAMAccountName)
Der Benutzeranmeldename (Prä-Windows 2000) darf keine der folgenden Zeichen enthalten: / \ [ ] : ; | = , + * ? < > @ und darf maximal 20 Zeichen lang sein. (Vordefinierte Richtlinie - Standardregeln zur Validierung von Objektnamen)
Benutzeranmeldename (Prä-Windows 2000):
- Muss angegeben werden.
- Muss in Übereinstimmung mit
<<
>>
Gehe zu
Schließen

Im Fenster können die folgenden Informationen angezeigt werden:

- **Richtlinienbeschreibung.** Bietet eine Kurzbeschreibung der Richtlinie.
- **Meldung.** Zeigt Details bezüglich des Problems an, wenn der angegebene Eigenschaftswert gegen die Richtlinie verstößt.

Sie können auf die Pfeile in der oberen linken Ecke klicken, um die Beschreibung anderer, für die angegebene Eigenschaft geltende Richtlinien anzuzeigen.

Der Abschnitt **Meldung** wird immer dann angezeigt, wenn der angegebene Eigenschaftswert gegen die Richtlinie verstößt. Die folgende Abbildung zeigt eine Situation, in der kein Wert für eine obligatorische Eigenschaft angegeben wurde.


Meldung
Das Feld "Benutzeranmeldename (Prä-Windows 2000)" darf nicht leer sein. Geben Sie einen Wert an und versuchen Sie es erneut.
Richtlinienbeschreibung
EIGENSCHAFT: Anmeldename (Prä-Windows 2000) (sAMAccountName)
Der Benutzeranmeldename (Prä-Windows 2000) darf keine der folgenden Zeichen enthalten: / \
Gehe zu
Schließen

Wenn Sie in diesem Fenster auf **Gehe zu** klicken, verschiebt die Konsole den Mauszeiger auf das Feld, das korrigiert werden muss. Sie können einen geeigneten Wert eingeben oder auswählen, um Ihre Eingabe zu korrigieren.

3

Regelbasierte administrative Ansichten

- Verwaltete Einheiten
- Administration verwalteter Einheiten
- Szenario: Implementieren der rollenbasierten Verwaltung über mehrere Organisationseinheiten hinweg
- Überlegungen bezüglich der Bereitstellung

Verwaltete Einheiten

Unternehmen entwerfen ihre auf Organisationseinheiten basierende Netzwerkstruktur meist anhand geografischer Grenzen oder Abteilungsgrenzen. Dies schränkt ihre Möglichkeiten ein, die Verwaltung außerhalb dieser Grenzen zu delegieren. Es können jedoch Situationen entstehen, in denen Objekten anders gruppiert werden müssen, als die auf Organisationseinheiten basierende Struktur vorsieht.

Active Directory bietet ein umfassendes Delegierungsmodell. Da der Delegierungsbereich jedoch anhand von Organisationseinheiten definiert ist, ist die verteilte Verwaltung in Active Directory entsprechend eingeschränkt.

In Active Directory ist es ohne Änderungen der Verzeichnisstruktur nicht möglich, Objekte so neu zu gruppieren, dass die neuen „Gruppen" die Vererbung für ihre Mitglieder beim Delegieren der Kontrolle oder Durchsetzen von Richtlinien unterstützen. Als Lösung für diese unflexible, auf Organisationseinheiten basierende Struktur ermöglicht Quest One ActiveRoles das Konfigurieren administrativer Ansichten, die alle Anforderungen an die Verzeichnisverwaltung erfüllen. Die administrativen Ansichten (verwalteten Einheiten) ermöglichen eine verteilte Verwaltung unabhängig von der Hierarchie der Organisationseinheiten.

Quest One ActiveRoles stellt also verwaltete Einheiten bereit: sicherbare, flexible, regelorientierte, administrative Ansichten. Verwaltete Einheiten stellen dynamische virtuelle Sammlungen von Objekten unterschiedlicher Typen dar. Verwaltete Einheiten können beliebige Verzeichnisobjekte einschließen, unabhängig von ihrem Standort im Netzwerk. Daher können Objekte in administrative Ansichten gruppiert werden, die von der auf Organisationseinheiten basierenden Struktur unabhängig sind.

Mit verwalteten Einheiten können Organisationen Organisationseinheitsstrukturen anhand geografischer Gegebenheiten implementieren, ihre Verwaltung jedoch nach funktionalen Kriterien verteilen. Beispielsweise können alle Benutzer in einer bestimmten Abteilung, unabhängig von ihrer Platzierung in unterschiedlichen Organisationseinheiten, zum Delegieren der Zugriffskontrolle und Durchsetzen administrativer Richtlinien in eine einzelne verwaltete Einheit gruppiert werden. Die Mitglieder dieser verwalteten Einheit bleiben dabei in ihren geografisch definierten Organisationseinheiten. Es entstehen keine Auswirkungen auf die Struktur der Organisationseinheiten.

Mit verwalteten Einheiten können Sie ein Unternehmen auf jede Weise strukturieren, ohne die zugrunde liegende Struktur aus Domänen und Organisationseinheiten zu ändern. Verwaltete Einheiten können Verzeichnisobjekte aus unterschiedlichen Domänenstrukturen und Gesamtstrukturen sowie aus anderen verwalteten Einheiten einschließen. Außerdem können unterschiedliche verwaltete Einheiten gemeinsame Mitglieder enthalten. Dank dieser Funktionen können Sie mit verwalteten Einheiten eine Umgebung erstellen, die sicher und leicht zu verwalten ist.

Funktionsweise verwalteter Einheiten

Mitgliedschaftsregeln bestimmen, ob ein Objekt Mitglied einer bestimmten verwalteten Einheit ist. Beispielsweise können Sie eine Mitgliedschaftsregel mit folgendem Inhalt angeben: Alle Benutzer der Organisationseinheit **A**, deren vollständige Namen mit **B** beginnen, gehören zu dieser verwalteten Einheit. Die Mitgliedschaftsregel wird dann als Abfrage implementiert, die die Organisationseinheit **A** nach Benutzern durchsucht, deren vollständige Namen mit **B** beginnen. Quest One ActiveRoles speichert die Abfrage in den Eigenschaften der verwalteten Einheit und führt sie bei jeder Erstellung oder Aktualisierung einer Liste von Mitgliedern der verwalteten Einheit aus.

Mit Quest One ActiveRoles können Berechtigungs- und Richtlinieneinstellungen auf der Ebene verwalteter Einheiten angegeben werden. Die Vererbung von Berechtigungs- und Richtlinieneinstellungen von der Ebene verwalteter Einheiten arbeitet nahtlos in der gesamten Active Directory-Umgebung.

Wenn die Umgebung geändert wird, werden auch die Mitgliedschaften von Objekten in verwalteten Einheiten gemäß der neuen Umgebung automatisch geändert. Dabei werden auch Berechtigungs- und Richtlinieneinstellungen für Objekte geändert. Verwaltete Einheiten werden dynamisch an Änderungen im Unternehmen angepasst. Dies vereinfacht die Verwaltung von Berechtigungs- und Richtlinieneinstellungen für Verzeichnisobjekte.

Jede verwaltetet Einheit stellt einen benutzerfreundlichen Bereich für die delegierte Verwaltung bereit. Delegierte Administratoren müssen die Hierarchie von Organisationseinheiten nicht mehr nach verwalteten Objekten durchsuchen. Mit Quest One ActiveRoles kann die administrative Kontrolle über jede verwaltete Einheit an bestimmte Benutzer und Gruppen delegiert werden, genau wie die Kontrolle über Organisationseinheiten. Mit verwalteten Einheiten befinden sich alle Objekte, die ein delegierter Administrator verwaltet, an einem einzigen Ort.

Administration verwalteter Einheiten

In diesem Abschnitt wird die Administration verwalteter Einheiten mit der Quest One ActiveRoles-Konsole vorgestellt. Folgende Themen werden erörtert:

- Erstellen einer verwalteten Einheit
- Anzeigen der Mitglieder einer verwalteten Einheit
- Hinzufügen und Entfernen von Mitgliedern einer verwalteten Einheit
- Kopieren einer verwalteten Einheit
- Exportieren und Importieren einer verwalteten Einheit
- Umbenennen einer verwalteten Einheit
- Löschen einer verwalteten Einheit

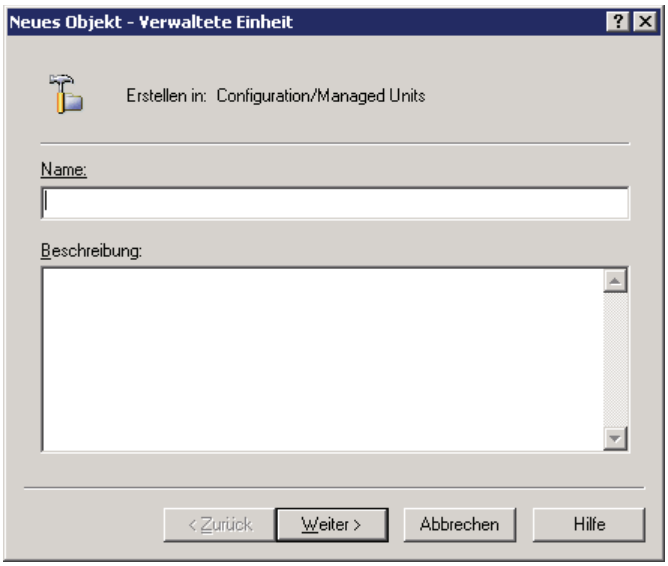
Erstellen einer verwalteten Einheit

Die Quest One ActiveRoles-Konsole stellt den Assistenten unter „Neues Objekt – verwaltete Einheit“ für die Erstellung verwalteter Einheiten bereit. Sie können den Assistenten vom Container **Verwaltete Einheiten** aus starten. Dieser befindet sich in der Konsolenstruktur unter **Konfiguration**: Klicken Sie mit der rechten Maustaste auf **Verwaltete Einheiten** in der Konsolenstruktur und wählen Sie **Erstellen | Verwaltete Einheit**.

Für die Administration einer großen Anzahl verwalteter Einheiten sollten Sie wie folgt Container erstellen, die nur angegebene verwaltete Einheiten enthalten, damit Sie sie leicht finden können: Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Verwaltete Einheiten** und wählen Sie **Erstellen | Verwaltete Einheiten-Container**. Verwenden Sie dann den Assistenten, um eine verwaltete Einheit in diesem Container zu erstellen: Klicken Sie mit der rechten Maustaste auf den Container und wählen Sie **Erstellen | Verwaltete Einheit**.

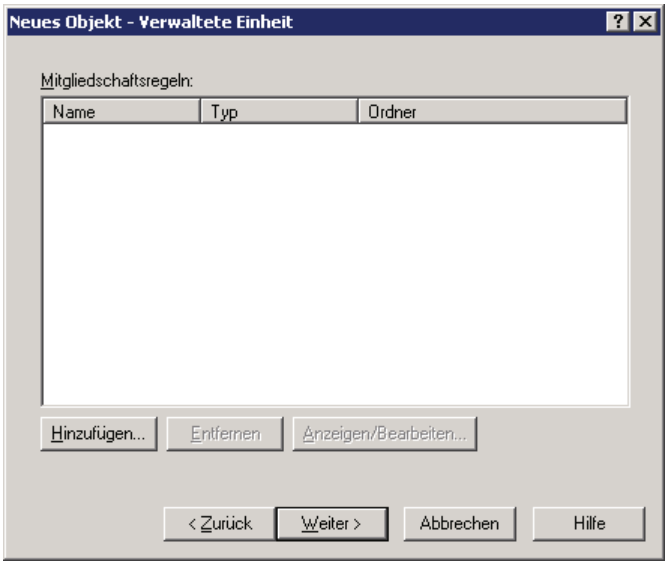
Nur Benutzer mit Administratorzugriff auf den Verwaltungsdienst (Mitglieder des ActiveRoles Admin-Kontos) dürfen verwaltete Einheiten erstellen. Weitere Informationen über das ActiveRoles Admin-Konto finden Sie im Handbuch *Quest One ActiveRoles – Erste Schritte*.

Die erste Seite des Assistenten entspricht der folgenden Abbildung.



Geben Sie auf dieser Seite den Namen und die Beschreibung für die verwaltete Einheit ein. Auf der Quest One ActiveRoles-Konsole werden im Bereich „Details" in der Liste der verwalteten Einheiten der Name und die Beschreibung angezeigt.

Klicken Sie auf **Weiter**. Die zweite Seite des Assistenten ähnelt der folgenden Abbildung.

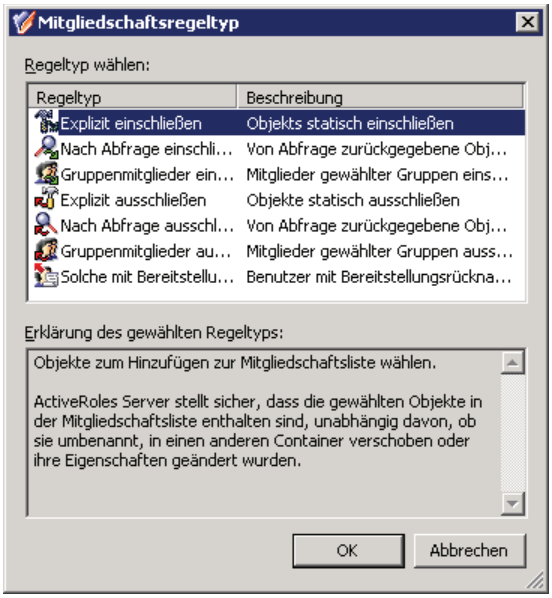


Auf dieser Seite können Sie angeben, welche Objekte in die verwaltete Einheit eingeschlossen werden sollen.

Die Mitgliedschaft in einer verwalteten Einheit wird durch Mitgliedschaftsregeln bestimmt. Mitglieder einer verwalteten Einheit sind die Objekte, die den in den Mitgliedschaftsregeln definierten Kriterien entsprechen. Eine Mitgliederliste kann dynamisch aktualisiert werden: Wenn Sie ein neues Objekt erstellen, das die Kriterien in der Mitgliedschaftsregel erfüllt, wird das Objekt automatisch in die verwaltete Einheit eingeschlossen. Wenn ein Objekt die in der Mitgliedschaftsregel angegebenen Kriterien nicht mehr erfüllt (weil es beispielsweise umbenannt oder verschoben wurde), wird es automatisch aus der Mitgliedschaftsliste ausgeschlossen.

Eine Mitgliedschaftsregel kann die Form einer Suchabfrage, einer Regel für die statische Einschließung und Ausschließung von Objekten sowie einer Regel für die Einschließung und Ausschließung von Gruppenmitgliedern haben.

Klicken Sie zum Angeben einer Mitgliedschaftsregel auf **Hinzufügen**. Hierdurch wird das Dialogfeld **Mitgliedschaftsregeltyp** angezeigt, das in der folgenden Abbildung dargestellt ist.



Wählen Sie in diesem Dialogfeld einen Typ von Mitgliedschaftsregel aus. Im unteren Feld finden Sie eine Beschreibung, die erläutert, welche Mitgliedschaftsregeln mit dem ausgewählten Typ erstellt werden können.

Der Regeltyp **Explizit einschließen** ermöglicht Ihnen, Objekte auszuwählen, die der verwalteten Einheit statisch hinzugefügt werden sollen. Wenn Sie einen Container (z.B. eine Organisationseinheit) auswählen, wird die gesamte Teilstruktur, deren Wurzel dieser Container ist, in die verwaltete Einheit eingeschlossen. Quest One ActiveRoles stellt sicher, dass die ausgewählten Objekte auch dann in die verwaltete Einheit eingeschlossen sind, wenn sie umbenannt oder in einen anderen Container verschoben werden oder wenn ihre Eigenschaften geändert werden.

Der Regeltyp **Explizit ausschließen** ermöglicht Ihnen, Objekte auszuwählen, die aus der verwalteten Einheit statisch ausgeschlossen werden sollen. Quest One ActiveRoles stellt sicher, dass die gewählten Objekte von der Mitgliedschaftsliste ausgeschlossen sind, unabhängig davon, ob sie umbenannt, verschoben oder ihre Eigenschaften geändert wurden. Da die Regel **Explizit ausschließen** Vorrang vor allen anderen Regeltypen hat, werden die ausgewählten Objekte auch dann aus der verwalteten Einheit ausgeschlossen, wenn eine andere Regel besagt, dass sie eingeschlossen werden sollen. Beachten Sie, dass dieser Regeltyp nur zum Ausschließen solcher Objekte verwendet werden kann, die mit einer der Aufnahmeregeln übereinstimmen.

Mit dem Regeltyp **Gruppenmitglieder einschließen** können Sie die Gruppen auswählen, deren Mitglieder Sie in die verwaltete Einheit einschließen möchten. Quest One ActiveRoles füllt die Mitgliedschaftsliste dynamisch mit den Objekten auf, die den ausgewählten Gruppen angehören. Wenn ein Objekt den ausgewählten Gruppen hinzugefügt oder aus ihnen entfernt wird, fügt Quest One ActiveRoles dieses Objekt der Mitgliedschaftsliste der verwalteten Einheit hinzu bzw. entfernt es aus ihr.

Mit dem Regeltyp **Gruppenmitglieder ausschließen** können Sie Gruppen auswählen, deren Mitglieder aus der verwalteten Einheit ausgeschlossen werden sollen. Quest One ActiveRoles stellt sicher, dass die Mitglieder der ausgewählten Gruppen aus der Mitgliedschaftsliste der verwalteten Einheit entfernt werden. Wenn ein Objekt in einer der gewählten Gruppen hinzugefügt wird, wird Quest One ActiveRoles dieses Objekt automatisch aus der Mitgliedschaftsliste entfernt. Beachten Sie, dass dieser Regeltyp nur zum Ausschließen solcher Objekte verwendet werden kann, die mit einer der Aufnahmeregeln übereinstimmen.

Mit dem Regeltyp **Nach Abfrage einschließen** können Sie Kriterien definieren, die die Objekte erfüllen müssen, um in die verwaltete Einheit eingeschlossen zu werden. Quest One ActiveRoles füllt die Mitgliedschaftsliste der Gruppe dynamisch mit den Objekten auf, die bestimmte Eigenschaften aufweisen. Wenn Sie ein Objekt erstellen oder seine Eigenschaften ändern, fügt Quest One ActiveRoles dieses Objekt der Mitgliedschaftsliste hinzu oder entfernt es aus dieser Liste, je nachdem, ob seine Eigenschaften die Kriterien erfüllen.

Mit dem Regeltyp **Nach Abfrage ausschließen** können Sie Kriterien definieren, die die Objekte erfüllen müssen, um aus der verwalteten Einheit ausgeschlossen zu werden. Quest One ActiveRoles stellt sicher, dass Objekte mit bestimmten Eigenschaften aus der Mitgliedschaftsliste ausgeschlossen werden. Quest One ActiveRoles entfernt Objekte automatisch aus der Mitgliedschaftsliste, wenn die Objekteigenschaften den definierten Kriterien entsprechen. Beachten Sie, dass dieser Regeltyp nur zum Ausschließen solcher Objekte verwendet werden kann, die mit einer der Aufnahmeregeln übereinstimmen.

Die Regel **Solche mit Bereitstellungsrücknahme** beibehalten dient zur Anpassung des Verhaltens verwalteter Einheiten in Bezug auf deprovisionierte Objekte wie etwa deprovisioniert Benutzer oder Gruppen. Nach der Deprovision eines Objekts wird das Objekt standardmäßig automatisch aus allen verwalteten Einheiten entfernt, in denen es Mitglied war. Wenn es notwendig ist, deprovisionierte Objekte in bestimmten verwalteten Einheiten beizubehalten, fügen Sie diesen verwalteten Einheiten die Regel **Deprovisioniert beibehalten** hinzu. Diese Regel führt dazu, dass die verwaltete Einheit sowohl die normalen als auch die deprovisionierten Objekte enthält, die den Mitgliedschaftsregeln für diese verwaltete Einheit entsprechen. Ohne diese Regel enthält die verwaltete Einheit keine deprovisionierten Objekte.

Beachten Sie, dass die Regeln, die Objekte aus einer verwalteten Einheit ausschließen, nur Auswirkungen auf die Objekte haben, die einer der Aufnahmeregeln für diese verwaltete Einheit entsprechen. Wenn beispielsweise ein Containerobjekt explizit in einer verwalteten Einheit enthalten ist, sind alle in diesem Container befindliche Objekte ebenfalls in der verwalteten Einheit enthalten und können nicht durch Anwendung von Ausschlussregeln ausgeschlossen werden. Eine Ausschlussregel kann nur verwendet werden, um den gesamten Container aus der verwalteten Einheit auszuschließen, da der Container das einzige Objekt ist, das einer Aufnahmeregel entspricht. Die sich im Container befindlichen Objekte entsprechen keiner Aufnahmeregel und sind daher von keinen Ausschlussregeln betroffen.

Wählen Sie im Dialogfeld **Mitgliedschaftsregeltyp** einen Regeltyp aus und klicken Sie dann auf **OK**.

Wenn Sie den Regeltyp **Explizit einschließen** oder **Explizit ausschließen** ausgewählt haben, wird das Dialogfeld **Objekte auswählen** angezeigt. Wählen Sie die Objekte aus, die Sie in die verwaltete Einheit einschließen oder aus ihr ausschließen möchten, klicken Sie auf **Hinzufügen** und dann auf **OK**.

Wenn Sie den Regeltyp **Gruppenmitglieder einschließen** oder **Gruppenmitglieder ausschließen** ausgewählt haben, wird das Dialogfeld **Objekte auswählen** angezeigt. Die Liste der Objekte in diesem Dialogfeld besteht aus Gruppen. Wählen Sie Gruppen aus, klicken Sie auf **Hinzufügen** und dann auf **OK**. Alle Mitglieder der ausgewählten Gruppen werden in die verwaltete Einheit eingeschlossen oder aus ihr ausgeschlossen.

Wenn Sie den Regeltyp **Nach Abfrage einschließen** oder **Nach Abfrage ausschließen** ausgewählt haben, wird das Dialogfeld **Mitgliedschaftsregel erstellen** angezeigt, das dem Dialogfeld **Suchen** ähnelt. Definieren Sie in diesem Dialogfeld die Kriterien, die Objekte erfüllen müssen, um in die verwaltete Einheit eingeschlossen oder aus ihr ausgeschlossen zu werden.

Nach dem Hinzufügen einer Mitgliedschaftsregel können Sie weitere Mitgliedschaftsregeln für dieselbe verwaltete Einheit hinzufügen.

Wenn Sie der verwalteten Einheit mehrere Mitgliedschaftsregeln hinzufügen und einige davon miteinander in Konflikt stehen, wird der Konflikt durch eine Regel gelöst, die die folgende Rangordnung definiert:

1. Explizit ausschließen
2. Explizit einschließen
3. Nach Abfrage ausschließen
4. Gruppenmitglieder ausschließen
5. Nach Abfrage einschließen
6. Gruppenmitglieder einschließen

Nach dieser Rangfolge hat z.B. die Regel **Explizit ausschließen** Vorrang vor allen anderen Regeltypen. Daher werden die ausgewählten Objekte auch dann aus der verwalteten Einheit ausgeschlossen, wenn eine andere Regel angibt, dass sie eingeschlossen werden sollen (beispielsweise die Objekte, die die in der Mitgliedschaftsregel **Nach Abfrage einschließen** definierten Kriterien erfüllen, oder zu einer Gruppe gehören, die in der Regel **Gruppenmitglieder einschließen** ausgewählt wurde).

Ein Ausschlussregeltyp kann nur zum Ausschließen solcher Objekte verwendet werden kann, die einer der Aufnahmeregeln entsprechen. Wenn beispielsweise eine bestimmte Organisationseinheit durch eine Aufnahmeregel in ein verwaltete Einheit aufgenommen wird, so werden alle in der Organisationseinheit enthaltenen untergeordneten Objekte ebenfalls in diese verwaltete Einheit aufgenommen. Es kann jedoch nur die gesamte Organisationseinheit und nicht ihre einzelnen untergeordneten Objekte aus der verwalteten Einheit ausgeschlossen werden.

Klicken Sie nach dem Auswählen von Mitgliedschaftsregeln auf **Weiter**. Die folgende Seite wird angezeigt:

Auf dieser Seite können Sie die Berechtigungs- und Richtlinieneinstellungen für die verwaltete Einheit angeben. Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und dann auf **Fertig stellen**. Ausführlichere Informationen über die Berechtigungseinstellungen finden Sie unter Anwenden von Zugriffsvorlagen weiter unten in diesem Dokument. Ausführlichere Informationen über die Richtlinieneinstellungen finden Sie unter Anwenden von Richtlinienobjekten weiter unten in diesem Dokument.

Verfahren zur Erstellung einer verwalteten Einheit

Gehen Sie folgendermaßen vor, um eine verwaltete Einheit zu erstellen:

1. Wählen Sie in der Konsolenstruktur unter **Quest One ActiveRoles | Configuration | Managed Units** den Ordner aus, zu dem Sie die verwaltete Einheit hinzufügen möchten.

   *Gehen Sie folgendermaßen vor, um einen neuen Ordner zu erstellen: Klicken Sie mit der rechten Maustaste auf **Managed Units** und wählen Sie **New | Managed Unit Container** aus. Auf die gleiche Weise können Sie einen Unterordner in einem Ordner erstellen: Klicken Sie mit der rechten Maustaste auf den Ordner und wählen Sie **New | Managed Unit Container** aus.*
2. Klicken Sie mit der rechten Maustaste auf den Ordner und wählen Sie **New | Managed Unit**, um den Assistenten „Neues Objekt – Verwaltete Einheit" zu starten.
3. Gehen Sie auf der ersten Seite des Assistenten wie folgt vor und klicken Sie dann auf **Weiter**:
   a) Geben Sie in das Feld **Name** den Namen der verwalteten Einheit ein.
   b) Geben Sie in das Feld **Beschreibung** nach Bedarf eine Beschreibung der verwalteten Einheit ein.
4. Klicken Sie auf der zweiten Seite des Assistenten auf **Hinzufügen**. Nun wird das Dialogfeld **Mitgliedschaftsregeltyp** angezeigt.
5. Wählen Sie den Typ der zu erstellenden Mitgliedschaftsregel aus und klicken Sie dann auf **OK**.
   - Um eine Regel zu erstellen, die statisch Mitglieder zur verwalteten Einheit hinzufügt, klicken Sie auf **Explizit einschließen**.
   - Um eine Regel zu erstellen, die statisch Mitglieder aus der verwalteten Einheit ausschließt, klicken Sie auf **Explizit ausschließen**.

- Um eine Regel zu erstellen, die alle Mitglieder einer bestimmten Gruppe zur verwalteten Einheit hinzufügt, klicken Sie auf **Gruppenmitglieder einschließen**.
- Um eine Regel zu erstellen, die alle Mitglieder einer bestimmten Gruppe aus der verwalteten Einheit ausschließt, klicken Sie auf **Gruppenmitglieder ausschließen**.
- Um eine Regel zu erstellen, die die verwaltete Einheit mit den Objekten füllt, die bestimmte Suchkriterien erfüllen, klicken Sie auf **Nach Abfrage einschließen**.
- Um eine Regel zu erstellen, die die verwaltete Einheit daran hindert, die Objekte aufzunehmen, die bestimmte Suchkriterien erfüllen, klicken Sie auf **Nach Abfrage ausschließen**.
- Um eine Regel zu erstellen, die verhindert, dass deprovisionierte Objekte wie etwa deprovisionierte Benutzer oder Gruppen aus der verwalteten Einheit entfernt werden, klicken Sie auf **Deprovisionierte beibehalten**.

*Wenn Sie den Regeltyp **Nach Abfrage einschließen** oder **Nach Abfrage ausschließen** in Schritt 5 ausgewählt haben, wird das Dialogfeld **Mitgliedschaftsregel erstellen** angezeigt. Ansonsten (mit Ausnahme des Regeltyps **Deprovisionierte beibehalten**) wird das Dialogfeld **Objekte auswählen** angezeigt.*

6. Schließen Sie das Dialogfeld **Mitgliedschaftsregel erstellen** oder **Objekte auswählen** entsprechend den weiter unten in diesem Hilfethema aufgeführten Verfahren ab.
7. Wiederholen Sie die Schritte 4 bis 6, bis Sie alle gewünschten Mitgliedschaftsregeln hinzugefügt haben. Klicken Sie dann auf **Weiter**.
8. Gehen Sie auf der nächsten Seite des Assistenten wie folgt vor und klicken Sie dann auf **Weiter**:
9. Klicken Sie auf **Sicherheit**, um Berechtigungseinstellungen für die verwaltete Einheit anzugeben.
10. Klicken Sie auf **Richtlinie**, um Richtlinieneinstellungen für die verwaltete Einheit anzugeben.

    Informationen über die Festlegung von Sicherheits- und Richtlinieneinstellungen finden Sie unter Verfahren zur Änderung der Berechtigungseinstellungen für eine verwaltete Einheit und Verfahren zur Änderung der Richtlinieneinstellungen für eine verwaltete Einheit weiter unten in diesem Dokument.

11. Klicken Sie auf der letzten Seite des Assistenten auf **Fertig stellen**.

Gehen Sie folgendermaßen vor, um das Dialogfeld „Mitgliedschaftsregel erstellen" abzuschließen:

1. Wählen Sie in der Liste **Suchen** die Klasse der Objekte aus, die die Mitgliedschaftsregel in die verwaltete Einheit aufnehmen oder aus ihr ausschließen soll. Wenn Sie zum Beispiel **Benutzer** auswählen, nimmt die Mitgliedschaftsregel die Benutzer auf bzw. schließt sie aus, die mit den von Ihnen angegebenen Bedingungen übereinstimmen.
2. Wählen Sie **in** der Liste In die Domäne oder den Ordner aus, die bzw. der die Objekte enthält, die die Mitgliedschaftsregel in die verwaltete Einheit aufnehmen oder aus ihr ausschließen soll. Wenn Sie zum Beispiel eine Organisationseinheit auswählen, dann nimmt die Mitgliedschaftsregel nur die Objekte auf bzw. schließt sie aus, die in der Organisationseinheit vorhanden sind.

   *Um Ordner zur Liste **In** hinzuzufügen, klicken Sie auf **Durchsuchen** und wählen Sie dann die Ordner im Dialogfeld **Container suchen** aus.*

3. Definieren Sie die Kriterien für die Mitgliedschaftsregel. Um zum Beispiel die Objekte aufzunehmen bzw. auszuschließen, deren Name mit dem Buchstaben „T" beginnen, geben Sie „T" in das Feld **Name** ein. Sie können ein Sternchen (*) als Platzhalter für jede beliebige Zeichenkette verwenden.
4. Klicken Sie optional auf **Regelvorschau**, um eine Liste der Objekte anzuzeigen, die mit den Kriterien übereinstimmen, die Sie definiert haben.
5. Klicken Sie auf **Regel hinzufügen**.

Gehen Sie folgendermaßen vor, um das Dialogfeld „Objekte auswählen" abzuschließen:

1. Klicken Sie in der Liste **Suchen in** auf die Domäne oder den Ordner, der die Objekte enthält, die Sie auswählen möchten. Um einen Ordner zur Liste hinzuzufügen, klicken Sie auf **Durchsuchen**.
2. Führen Sie einen der nachfolgend aufgeführten Schritte durch und klicken Sie dann auf **OK**
   - Doppelklicken Sie in der Liste der Objekte auf das Objekt, das Sie hinzufügen wollen.
   - Geben Sie in das untere Feld den vollständigen Namen oder einen Teil des Namens des Objekts ein, das Sie hinzufügen möchten. Klicken Sie anschließend auf **Namen prüfen**.

- Sie können auch den Befehl **Eigenschaften** verwenden, um Mitgliedschaftsregeln zu einer vorhandenen verwalteten Einheit hinzuzufügen bzw. aus ihr zu entfernen: Klicken Sie mit der rechten Maustaste auf die verwaltete Einheit, klicken Sie auf **Eigenschaften** und klicken Sie dann auf die Registerkarte **Mitgliedschaftsregeln** im Dialogfeld **Eigenschaften**.
- Informationen über die Anzeige der Mitgliederliste einer verwalteten Einheit finden Sie unter Anzeigen der Mitglieder einer verwalteten Einheit weiter unten in diesem Dokument.
- Das Dialogfeld **Mitgliedschaftsregel erstellen** ist identisch mit dem Dialogfeld **Suchen**, das Sie für die Suche nach Objekten im Verzeichnis verwenden. Wenn Sie Ihre Suchkriterien angegeben haben, speichert die Funktion **Regel hinzufügen** diese als eine Mitgliedschaftsregel. Weitere Informationen bezüglich der Festlegung von Suchkriterien finden Sie unter Suchen nach Objekten weiter oben in diesem Dokument.
- Die Liste **Suchen** umfasst den Eintrag **Benutzerdefinierte Suche**. Durch Auswahl des Eintrags **Benutzerdefinierte Suche** wird die Registerkarte angezeigt, in der Sie mittels erweiterter Optionen benutzerdefinierte Mitgliedschaftsregeln erstellen sowie mittels des LDAP-Protokolls (Lightweight Directory Access Protocol), des Haupt-Zugriffsprotokolls für Active Directory, erweiterte Mitgliedschaftsregeln erstellen können. Weitere Informationen über die Verwendung von erweiterten Suchoptionen finden Sie unter Verfahren zum Anlegen einer benutzerdefinierten Suche und Verfahren zum Verwenden von erweiterten Optionen für die Suche weiter oben in diesem Dokument.

Verfahren zur Änderung der Eigenschaften einer verwalteten Einheit

So ändern Sie Eigenschaften einer verwalteten Einheit:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Quest One ActiveRoles | Configuration | Managed Units**.
2. Suchen Sie unter **Managed Units** die verwaltete Einheit, die Sie ändern möchten, klicken Sie mit der rechten Maustaste darauf und klicken Sie dann auf **Eigenschaften**.
3. Verwenden Sie die Registerkarten im Dialogfeld **Eigenschaften**, um die Eigenschaften der verwalteten Einheit anzuzeigen oder zu ändern.
4. Klicken Sie abschließend auf **OK**.

- Die Registerkarte **Mitgliedschaftsregeln** zeigt eine Liste der Mitgliedschaftsregeln für eine bestimmte verwaltete Einheit an. Sie können bei Bedarf Mitgliedschaftsregeln hinzufügen, entfernen oder ändern. Ausführlichere Informationen finden Sie unter Hinzufügen und Entfernen von Mitgliedern einer verwalteten Einheit weiter unten in diesem Dokument.
- Auf der Registerkarte **Verwaltung** können Sie die Option **Richtlinie** wählen, um Richtlinienobjekt verknüpfungen hinzuzufügen und zu entfernen, die festlegen, welche administrativen Richtlinien für die verwaltete Einheit erzwungen werden. Ausführlichere Informationen finden Sie unter Verfahren zur Änderung der Richtlinieneinstellungen für eine verwaltete Einheit weiter unten in diesem Dokument.
- Auf der Registerkarte **Verwaltung** können Sie die Option **Sicherheit** wählen, um Zugriffsvorlagenverknüpfungen hinzuzufügen und zu entfernen, die Trustees und deren Berechtigungen für die verwaltete Einheit festlegen. Ausführlichere Informationen finden Sie unter Verfahren zur Änderung der Berechtigungseinstellungen für eine verwaltete Einheit weiter unten in diesem Dokument.

Verfahren zur Änderung der Berechtigungseinstellungen für eine verwaltete Einheit

So ändern Sie Berechtigungseinstellungen an einer verwalteten Einheit:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Quest One ActiveRoles | Configuration | Managed Units**.
2. Suchen Sie unter **Managed Units** die verwaltete Einheit, die Sie ändern möchten, klicken Sie mit der rechten Maustaste darauf und klicken Sie dann auf **Kontrolle delegieren**.
3. Tun Sie im Dialogfeld **Quest One ActiveRoles-Sicherheit** Folgendes:
   - Um Berechtigungen zur verwalteten Einheit hinzuzufügen, klicken Sie auf **Hinzufügen** und befolgen Sie die Anweisungen des Assistenten zum Delegieren der Kontrolle, um eine Zugriffsvorlagenverknüpfung zu erstellen. Informationen über die Verwendung des Assistenten zum Delegieren der Kontrolle finden Sie unter Anwenden von Zugriffsvorlagen weiter unten in diesem Dokument.
   - Um Berechtigungen aus der verwalteten Einheit zu entfernen, wählen Sie die Zugriffsvorlagenverknüpfungen aus der Liste aus und klicken Sie dann auf **Entfernen**. Alternativ dazu können Sie die Berechtigungen durch Deaktivieren der Zugriffsvorlagen verknüpfungen zurücknehmen: Wählen Sie eine oder mehrere Verknüpfungen aus und klicken Sie dann auf **Deaktivieren**.
   - Um die Eigenschaften einer Zugriffsvorlagenverknüpfung für die verwaltete Einheit anzuzeigen oder zu ändern, wählen Sie die Verknüpfung in der Liste aus und klicken Sie dann auf **Anzeigen/Bearbeiten**.
   - Um eine Zugriffsvorlagenverknüpfung so zu ändern, dass die von der Verknüpfung definierten Berechtigungen auch zu Active Directory hinzugefügt werden, wählen Sie die Verknüpfung in der Liste aus und klicken Sie dann auf **Mit AD synchronisieren**.
4. Klicken Sie auf **OK**, um das Dialogfeld **Quest One ActiveRoles-Sicherheit** zu schließen.

- Das Dialogfeld **Quest One ActiveRoles-Sicherheit** zeigt eine Liste der Zugriffsvorlagenverknüpfungen an, wobei jeder Listeneintrag einen Trustee und die Zugriffsvorlage angibt, die verwendet wird, um die Berechtigungen des Trustees anzugeben.
- Standardmäßig zeigt die Liste der Zugriffsvorlagenverknüpfungen alle Verknüpfungen an, die die Berechtigungseinstellungen für die verwaltete Einheit festlegen, und zwar unabhängig davon, ob eine Verknüpfung für die verwaltete Einheit selbst oder für einen Container, in dem sich die verwaltete Einheit befindet, erstellt wurde. Um die Anzeige der Liste zu ändern, deaktivieren Sie das Kontrollkästchen **Vererbung anzeigen**.
- Eine Zugriffsvorlagenverknüpfung kann aus einer verwalteten Einheit entfernt werden, wenn die Verknüpfung für diese verwaltete Einheit erstellt wurde. Nur die Verknüpfungen, die diese Bedingung erfüllen, werden angezeigt, wenn Sie das Kontrollkästchen **Vererbung anzeigen** deaktivieren. So können Sie sie entfernen, indem Sie auf **Entfernen** klicken.
- Sie können auch die erweiterte Detailanzeige verwenden, um Zugriffsvorlagenverknüpfungen für eine verwaltete Einheit anzuzeigen, hinzuzufügen, zu entfernen oder zu ändern: Wählen Sie die verwaltete Einheit aus und klicken Sie dann auf der Registerkarte **ActiveRoles-Sicherheit** in der erweiterten Detailanzeige mit der rechten Maustaste auf eine Zugriffsvorlagenverknüpfung oder einen freien Bereich und verwenden Sie die Befehle im Kontextmenü. Informationen über die erweiterte Detailanzeige finden Sie unter Erweiterter Bereich weiter oben in diesem Dokument.

Verfahren zur Änderung der Richtlinieneinstellungen für eine verwaltete Einheit

So ändern Sie Richtlinieneinstellungen an einer verwalteten Einheit:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Quest One ActiveRoles | Configuration | Managed Units**.
2. Suchen Sie unter **Managed Units** die verwaltete Einheit, die Sie ändern möchten, klicken Sie mit der rechten Maustaste darauf und klicken Sie dann auf **Richtlinie erzwingen**.
3. Nehmen Sie im Dialogfeld **Quest One ActiveRoles-Richtlinie** Folgendes vor:
   - Um Richtlinien zur verwaltete Einheit hinzuzufügen, klicken Sie auf **Hinzufügen** und wählen Sie das Richtlinienobjekt, das die Richtlinien definiert. Sie können mehrere Richtlinienobjekte gleichzeitig auswählen.
   - Um Richtlinien aus der verwaltete Einheit zu entfernen, wählen Sie das Richtlinienobjekt aus, das die Richtlinien definiert, und klicken Sie dann auf **Entfernen**. Alternativ dazu können Sie die Auswirkungen eines Richtlinienobjekts auf die verwaltete Einheit unterbinden, indem Sie das Kontrollkästchen **Gesperrt** neben dem Namen des Richtlinienobjekts aktivieren.
   - Um Richtlinien zu ändern, wählen Sie das Richtlinienobjekt aus, das die Richtlinien definiert, und klicken Sie dann auf **Anzeigen/Bearbeiten**.
4. Klicken Sie auf **OK**, um das Dialogfeld **Quest One ActiveRoles-Richtlinie** zu schließen.

- Das Dialogfeld **Quest One ActiveRoles-Richtlinie** listet alle Richtlinienobjekte auf, die die Richtlinieneinstellungen für die verwaltete Einheit festlegen, und zwar unabhängig davon, ob ein Richtlinienobjekte zur verwalteten Einheit selbst oder für einen Container, in dem sich die verwaltete Einheit befindet, hinzugefügt wurde. Sie können eine Liste der Richtlinienobjekte anzeigen, die direkt zur verwalteten Einheit hinzugefügt wurden: Klicken Sie auf **Erweitert** und deaktivieren Sie dann das Kontrollkästchen **Vererbung anzeigen**.
- Es können nur die Richtlinienobjekte entfernt werden, die direkt zur verwalteten Einheit hinzugefügt wurden. Selbst wenn die Schaltfläche **Entfernen** nicht verfügbar ist, können Sie das Kontrollkästchen **Gesperrt** aktivieren. Auf diese Weise können Sie die Auswirkungen des Richtlinienobjekts auf die verwaltete Einheit unterbinden. Sie können jederzeit die Auswirkungen des Richtlinienobjekts auf die verwaltete Einheit wiederherstellen, indem Sie das Kontrollkästchen **Gesperrt** deaktivieren.
- Sie können auch die erweiterte Detailanzeige verwenden, um Richtlinienobjekte hinzuzufügen, zu entfernen, zu sperren oder zu ändern, die die Richtlinieneinstellungen für eine verwaltete Einheit definieren: Wählen Sie die verwaltete Einheit aus und klicken Sie dann auf der Registerkarte **ActiveRoles-Richtlinie** in der erweiterten Detailanzeige mit der rechten Maustaste auf ein Richtlinienobjekt oder einen freien Bereich und verwenden Sie die Befehle im Kontextmenü. Informationen über die erweiterte Detailanzeige finden Sie unter Erweiterter Bereich weiter oben in diesem Dokument.

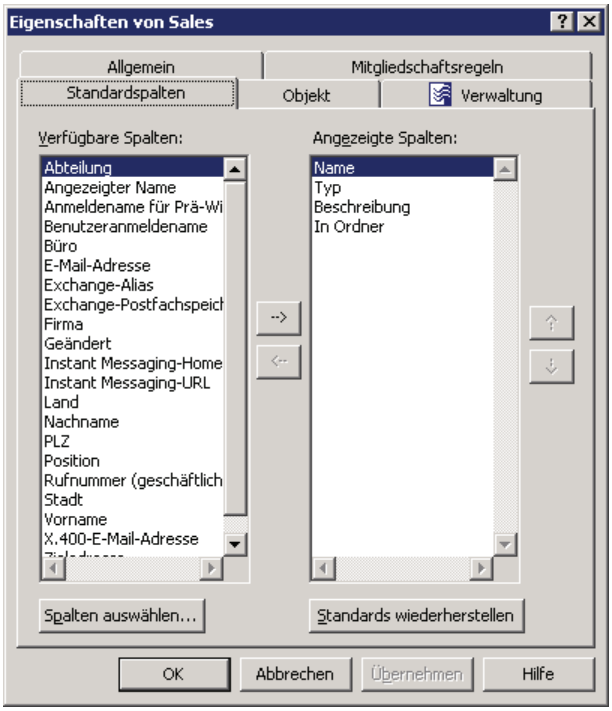
Anzeigen der Mitglieder einer verwalteten Einheit

Die Mitglieder einer verwalteten Einheit sind Objekte, die den Kriterien entsprechen, die in den Mitgliedschaftsregeln für die verwaltete Einheit angegeben sind.

Um die Mitglieder einer verwalteten Einheit anzuzeigen, erweitern Sie in der Konsolenstruktur **Configuration/Managed Units** und klicken Sie dann auf eine verwaltete Einheit. Im Bereich „Details" werden nun die Mitglieder der verwalteten Einheit angezeigt.

Sie können für jede verwaltete Einheit eine eigene Spaltengruppe vorher festlegen, die im Bereich „Details" angezeigt werden soll. So können Sie administrative Ansichten für einzelne verwaltete Einheiten festlegen.

Um für eine bestimmte verwaltete Einheit Spalten im Bereich „Details" vorher festzulegen, klicken Sie mit der rechten Maustaste auf die verwaltete Einheit, klicken Sie auf **Eigenschaften** und öffnen Sie die Registerkarte **Standardspalten**. Die Registerkarte ähnelt der folgenden Abbildung:



Um eine anzuzeigende Spalte hinzuzufügen, doppelklicken Sie in der Liste **Verfügbare Spalten** auf ihren Namen. Um Spalten zur Liste **Verfügbare Spalten** hinzuzufügen, klicken Sie auf **Spalten auswählen**. Im Dialogfeld **Spalten auswählen** können Sie Spalten auswählen und erforderlichenfalls die Namen ändern, die in den Spaltenüberschriften angezeigt werden.

Durch Doppelklicken auf einen Spaltennamen unter **Verfügbare Spalten** wird der Name zur Liste **Angezeigte Spalten** hinzugefügt. Klicken Sie auf **OK**. Die neue Spalte wird nach dem Aktualisieren der Ansicht im Bereich „Details" angezeigt. Klicken Sie mit der rechten Maustaste in der Konsolenstruktur auf **Managed Units** und klicken Sie dann auf **Aktualisieren**; wählen Sie dann die verwaltete Einheit in der Konsolenstruktur aus: Im Bereich „Details" wird die neue Spalte angezeigt.

Verfahren zur Anzeige der Mitglieder einer verwalteten Einheit

So zeigen Sie die Mitglieder einer verwalteten Einheit an:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Quest One ActiveRoles | Configuration | Managed Units**.
2. Suchen Sie unter **Managed Units** die verwaltete Einheit und wählen Sie sie aus.
   Im Bereich „Details" werden nun die Mitglieder der verwalteten Einheit aufgelistet.

Gehen Sie folgendermaßen vor, um die Liste der Mitglieder der verwalteten Einheit im Bereich „Details" anzupassen:

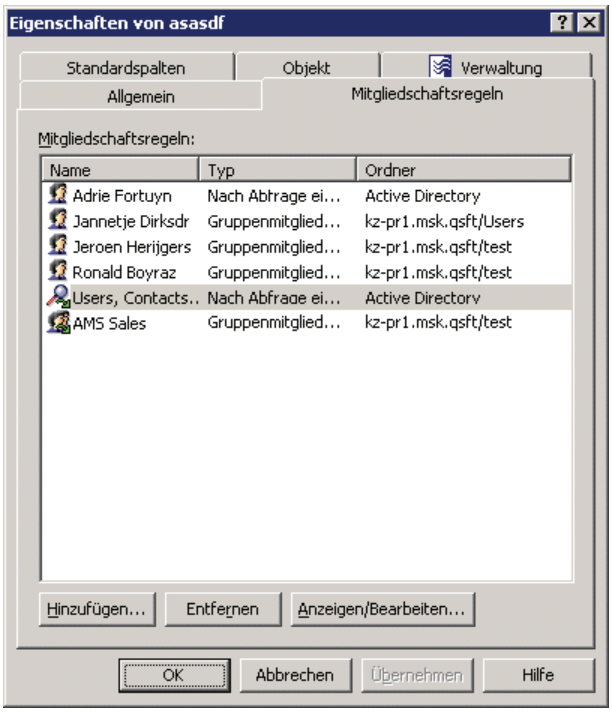
1. Klicken Sie mit der rechten Maustaste auf die verwaltete Einheit und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie im Dialogfeld **Eigenschaften** auf die Registerkarte **Standardspalten**.
3. Fügen Sie auf der Registerkarte **Standardspalten** Spaltennamen zur Liste **Angezeigte Spalten** hinzu bzw. entfernen Sie sie aus der Liste.
4. Klicken Sie auf **OK**.

- Für jede verwaltete Einheit kann eine individuelle Liste der im Bereich „Details" anzuzeigenden Standardspalten konfiguriert werden. Das heißt, dass Sie die Anpassung für jede verwaltete Einheit individuell durchführen können.
- Sie können die Liste **Angezeigte Spalten** füllen, indem Sie in der Liste **Verfügbare Spalten** auf der Registerkarte **Standardspalten** auf die Spaltennamen doppelklicken. Sie können Spalten entfernen, indem Sie in der Liste **Angezeigte Spalten** auf die Spaltennamen doppelklicken.
- Um Spaltenelemente zur Liste **Verfügbare Spalten** hinzuzufügen, klicken Sie auf **Spalten auswählen**. Im Dialogfeld Spalten auswählen können Sie **Spalten auswählen** und erforderlichenfalls die Spaltennamen ändern.
- Damit Ihre Änderungen an der Liste **Angezeigte Spalten** berücksichtigt werden, muss der Bereich „Details" aktualisiert werden: Klicken Sie mit der rechten Maustaste in der Konsolenstruktur auf **Managed Units** und klicken Sie dann auf **Aktualisieren**.

Hinzufügen und Entfernen von Mitgliedern einer verwalteten Einheit

Die Mitglieder einer verwalteten Einheit werden durch Mitgliedschaftsregeln definiert. Zum Hinzufügen oder Entfernen von Mitgliedern einer verwalteten Einheit müssen Sie daher Mitgliedschaftsregeln hinzufügen, löschen oder ändern.

Um Mitgliedschaftsregeln für eine verwaltete Einheit hinzuzufügen, zu löschen oder zu ändern, rufen Sie das Dialogfeld **Eigenschaften** für die entsprechende verwaltete Einheit auf und klicken Sie dann auf die Registerkarte **Mitgliedschaftsregeln**. Die Registerkarte ähnelt der folgenden Abbildung:



Auf der Registerkarte **Mitgliedschaftsregeln** wird eine Liste von Mitgliedschaftsregeln angezeigt. Dabei zeigt jeder Eintrag den Namen, Typ und Gültigkeitsbereich der Regel an.

Klicken Sie zum Hinzufügen einer Mitgliedschaftsregel auf **Hinzufügen**. Daraufhin wird das Dialogfeld **Mitgliedschaftsregeltyp** angezeigt, das weiter oben in diesem Kapitel beschrieben ist (siehe Erstellen einer verwalteten Einheit).

Um eine **Mitgliedschaftsregel** zu ändern, wählen Sie sie aus der Liste Mitgliedschaftsregeln aus und klicken Sie dann auf **Anzeigen/Bearbeiten**. Nur abfragebasierte Regeln können auf diese Weise geändert werden. Wenn Sie eine Regel eines anderen Typs auswählen, ist die Schaltfläche **Anzeigen/Bearbeiten** nicht verfügbar.

Um eine **Mitgliedschaftsregel** zu löschen, wählen Sie sie in der Liste Mitgliedschaftsregeln aus und klicken Sie dann auf **Entfernen**.

Wenn Sie Mitgliedschaftsregeln hinzufügen, ändern oder löschen, wird auch die Mitgliedschaftsliste der verwalteten Einheit geändert.

Verfahren zum Hinzufügen von Mitgliedschaftsregeln zu einer verwalteten Einheit

So fügen Sie eine Mitgliedschaftsregel zu einer verwalteten Einheit hinzu:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Quest One ActiveRoles | Configuration | Managed Units**.
2. Suchen Sie unter **Managed Units** die verwaltete Einheit, die Sie ändern möchten, klicken Sie mit der rechten Maustaste darauf und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf der Registerkarte **Mitgliedschaftsregeln** auf **Hinzufügen**. Nun wird das Dialogfeld **Mitgliedschaftsregeltyp** angezeigt.
4. Wählen Sie die Art der Mitgliedschaftsregel aus, die Sie erstellen möchten. Führen Sie einen der nachfolgend aufgeführten Schritte durch und klicken Sie dann auf **OK**
   - Um eine Regel zu erstellen, die statisch Mitglieder zur verwalteten Einheit hinzufügt, klicken Sie auf **Explizit einschließen**.
   - Um eine Regel zu erstellen, die statisch Mitglieder aus der verwalteten Einheit ausschließt, klicken Sie auf **Explizit ausschließen**.
   - Um eine Regel zu erstellen, die alle Mitglieder einer bestimmten Gruppe zur verwalteten Einheit hinzufügt, klicken Sie auf **Gruppenmitglieder einschließen**.
   - Um eine Regel zu erstellen, die alle Mitglieder einer bestimmten Gruppe aus der verwalteten Einheit ausschließt, klicken Sie auf **Gruppenmitglieder ausschließen**.
   - Um eine Regel zu erstellen, die die verwaltete Einheit mit den Objekten füllt, die bestimmte Suchkriterien erfüllen, klicken Sie auf **Nach Abfrage einschließen**.
   - Um eine Regel zu erstellen, die die verwaltete Einheit daran hindert, die Objekte aufzunehmen, die bestimmte Suchkriterien erfüllen, klicken Sie auf **Nach Abfrage ausschließen**.
   - Um eine Regel zu erstellen, die verhindert, dass deprovisionierte Objekte wie etwa deprovisionierte Benutzer oder Gruppen aus der verwalteten Einheit entfernt werden, klicken Sie auf **Deprovisionierte beibehalten**.

   *Wenn Sie den Regeltyp **Nach Abfrage einschließen** oder **Nach Abfrage ausschließen** in Schritt 5 ausgewählt haben, wird das Dialogfeld **Mitgliedschaftsregel erstellen** angezeigt. Ansonsten (mit Ausnahme des Regeltyps **Deprovisionierte beibehalten**) wird das Dialogfeld **Objekte auswählen** angezeigt.*
5. Schließen Sie das Dialogfeld **Mitgliedschaftsregel erstellen** oder **Objekte auswählen** entsprechend den weiter unten in diesem Hilfethema aufgeführten Verfahren ab.
6. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** zu schließen.

Gehen Sie folgendermaßen vor, um das Dialogfeld „Mitgliedschaftsregel erstellen" abzuschließen:

1. Wählen Sie in der Liste **Suchen** die Klasse der Objekte aus, die die Mitgliedschaftsregel in die verwaltete Einheit aufnehmen oder aus ihr ausschließen soll. Wenn Sie zum Beispiel **Benutzer** auswählen, nimmt die Mitgliedschaftsregel die Benutzer auf bzw. schließt sie aus, die mit den von Ihnen angegebenen Bedingungen übereinstimmen.
2. Wählen Sie **in** der Liste In die Domäne oder den Ordner aus, die bzw. der die Objekte enthält, die die Mitgliedschaftsregel in die verwaltete Einheit aufnehmen oder aus ihr ausschließen soll. Wenn Sie zum Beispiel eine Organisationseinheit auswählen, dann nimmt die Mitgliedschaftsregel nur die Objekte auf bzw. schließt sie aus, die in der Organisationseinheit vorhanden sind.

   *Um Ordner zur Liste **In** hinzuzufügen, klicken Sie auf **Durchsuchen** und wählen Sie dann die Ordner im Dialogfeld **Container suchen** aus.*

3. Definieren Sie die Kriterien für die Mitgliedschaftsregel. Um zum Beispiel die Objekte aufzunehmen bzw. auszuschließen, deren Name mit dem Buchstaben „T" beginnen, geben Sie „T" in das Feld **Name** ein. Sie können ein Sternchen (*) als Platzhalter für jede beliebige Zeichenkette verwenden.
4. Klicken Sie optional auf **Regelvorschau**, um eine Liste der Objekte anzuzeigen, die mit den Kriterien übereinstimmen, die Sie definiert haben.
5. Klicken Sie auf **Regel hinzufügen**.

Gehen Sie folgendermaßen vor, um das Dialogfeld „Objekt auswählen" abzuschließen:

1. Klicken Sie in der Liste **Suchen in** auf die Domäne oder den Ordner, der die Objekte enthält, die Sie auswählen möchten. Um einen Ordner zur Liste hinzuzufügen, klicken Sie auf **Durchsuchen**.
2. Führen Sie einen der nachfolgend aufgeführten Schritte durch und klicken Sie dann auf **OK**
   - Doppelklicken Sie in der Liste der Objekte auf das Objekt, das Sie hinzufügen wollen.
   - Geben Sie in das untere Feld den vollständigen Namen oder einen Teil des Namens des Objekts ein, das Sie hinzufügen möchten. Klicken Sie anschließend auf **Namen prüfen**.

- Die einzige Möglichkeit, verwaltete Einheiten zu füllen, besteht darin, Mitgliedschaftsregeln hinzuzufügen. Die Mitglieder einer verwalteten Einheit sind die Objekte, die mit den von den Mitgliedschaftsregeln definierten Kriterien übereinstimmen.
- Um Mitglieder einer verwalteten Einheit anzuzeigen, klicken Sie in der Konsolenstruktur auf die verwaltete Einheit. Im Bereich „Details" werden nun die Mitglieder der verwalteten Einheit angezeigt.
- Das Dialogfeld **Mitgliedschaftsregel erstellen** ist identisch mit dem Dialogfeld **Suchen**, das Sie für die Suche nach Objekten im Verzeichnis verwenden. Wenn Sie Ihre Suchkriterien angegeben haben, ermöglicht Ihnen Quest One ActiveRoles, diese als eine Mitgliedschaftsregel zu speichern, wodurch erzwungen wird, dass die Mitgliedschaftsliste die Objekte aufnimmt, die mit den Suchkriterien übereinstimmen. Anweisungen bezüglich der Festlegung von Suchkriterien im Dialogfeld **Mitgliedschaftsregel erstellen** finden Sie unter Suchen nach Objekten weiter oben in diesem Dokument.
- Die Liste **Suchen** umfasst den Eintrag **Benutzerdefinierte Suche**. Durch Auswahl des Eintrags **Benutzerdefinierte Suche** wird die Registerkarte angezeigt, in der Sie mittels erweiterter Optionen benutzerdefinierte Mitgliedschaftsregeln erstellen sowie mittels des LDAP-Protokolls (Lightweight Directory Access Protocol), des Haupt-Zugriffsprotokolls für Active Directory, erweiterte Mitgliedschaftsregeln erstellen können. Weitere Informationen über die Verwendung von erweiterten Suchoptionen finden Sie unter Verfahren zum Anlegen einer benutzerdefinierten Suche und Verfahren zum Verwenden von erweiterten Optionen für die Suche weiter oben in diesem Dokument.

Verfahren zum Entfernen von Mitgliedschaftsregeln aus einer verwalteten Einheit

So entfernen Sie eine Mitgliedschaftsregel aus einer verwalteten Einheit:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Quest One ActiveRoles | Configuration | Managed Units**.
2. Suchen Sie unter **Managed Units** die verwaltete Einheit, die Sie ändern möchten, klicken Sie mit der rechten Maustaste darauf und klicken Sie dann auf **Eigenschaften**.
3. Wählen Sie auf der Registerkarte **Mitgliedschaftsregeln** die Mitgliedschaftsregel und klicken dann auf **Entfernen**.

Verfahren zum Aufnehmen von Mitgliedern in eine verwaltete Einheit

So nehmen Sie ein Mitglied in eine verwaltete Einheit auf:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Quest One ActiveRoles | Configuration | Managed Units**.
2. Suchen Sie unter **Managed Units** die verwaltete Einheit, die Sie ändern möchten, klicken Sie mit der rechten Maustaste darauf und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf der Registerkarte **Mitgliedschaftsregeln** auf **Hinzufügen**. Das Dialogfeld **Mitgliedschaftsregeltyp** wird angezeigt.
4. Klicken Sie im Dialogfeld **Mitgliedschaftsregeltyp** auf **Explizit einschließen** und klicken Sie dann auf **OK**. Das Dialogfeld **Objekte auswählen** wird angezeigt.
5. Verwenden Sie das Dialogfeld **Objekte auswählen**, um die Objekte auszuwählen, die explizit in die verwaltete Einheit aufgenommen werden sollen.

   Allgemeine Anweisungen bezüglich der Konfiguration von Mitgliedschaftsregeln finden Sie unter Verfahren zum Hinzufügen von Mitgliedschaftsregeln zu einer verwalteten Einheit weiter oben in diesem Dokument.
6. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** zu schließen.

Verfahren zum Ausschließen von Mitgliedern aus einer verwalteten Einheit

So schließen Sie ein Mitglied aus einer verwalteten Einheit aus:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Quest One ActiveRoles | Configuration | Managed Units**.
2. Suchen Sie unter **Managed Units** die verwaltete Einheit, die Sie ändern möchten, klicken Sie mit der rechten Maustaste darauf und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf der Registerkarte **Mitgliedschaftsregeln** auf **Hinzufügen**. Das Dialogfeld **Mitgliedschaftsregeltyp** wird angezeigt.
4. Klicken Sie im Dialogfeld **Mitgliedschaftsregeltyp** auf **Explizit ausschließen** und klicken Sie dann auf **OK**. Das Dialogfeld **Objekte auswählen** wird angezeigt.
5. Verwenden Sie das Dialogfeld **Objekte auswählen**, um die Objekte auszuwählen, die explizit aus der verwalteten Einheit ausgeschlossen werden sollen.

   Allgemeine Anweisungen bezüglich der Konfiguration von Mitgliedschaftsregeln finden Sie unter Verfahren zum Hinzufügen von Mitgliedschaftsregeln zu einer verwalteten Einheit weiter oben in diesem Dokument.
6. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** zu schließen.

Verfahren zum Hinzufügen von Gruppenmitgliedern zu einer verwalteten Einheit

So fügen Sie Gruppenmitglieder zu einer verwalteten Einheit hinzu:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Quest One ActiveRoles | Configuration | Managed Units**.
2. Suchen Sie unter **Managed Units** die verwaltete Einheit, die Sie ändern möchten, klicken Sie mit der rechten Maustaste darauf und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf der Registerkarte **Mitgliedschaftsregeln** auf **Hinzufügen**. Das Dialogfeld **Mitgliedschaftsregeltyp** wird angezeigt.
4. Klicken Sie im Dialogfeld **Mitgliedschaftsregeltyp** auf **Gruppenmitglieder einschließen** und klicken Sie dann auf **OK**. Das Dialogfeld **Objekte auswählen** wird angezeigt.

5. Verwenden Sie das Dialogfeld **Objekte auswählen**, um die Gruppen auszuwählen, deren Mitglieder in die verwaltete Einheit aufgenommen werden sollen.

   Allgemeine Anweisungen bezüglich der Konfiguration von Mitgliedschaftsregeln finden Sie unter Verfahren zum Hinzufügen von Mitgliedschaftsregeln zu einer verwalteten Einheit weiter oben in diesem Dokument.

6. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** zu schließen.

Verfahren zum Entfernen von Gruppenmitgliedern aus einer verwalteten Einheit

So entfernen Sie Gruppenmitglieder aus einer verwalteten Einheit:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Quest One ActiveRoles | Configuration | Managed Units**.
2. Suchen Sie unter **Managed Units** die verwaltete Einheit, die Sie ändern möchten, klicken Sie mit der rechten Maustaste darauf und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf der Registerkarte **Mitgliedschaftsregeln** auf **Hinzufügen**. Das Dialogfeld **Mitgliedschaftsregeltyp** wird angezeigt.
4. Klicken Sie im Dialogfeld **Mitgliedschaftsregeltyp** auf **Gruppenmitglieder ausschließen** und klicken Sie dann auf **OK**. Das Dialogfeld **Objekte auswählen** wird angezeigt.
5. Verwenden Sie das Dialogfeld **Objekte auswählen**, um die Gruppen auszuwählen, deren Mitglieder aus der verwalteten Einheit ausgeschlossen werden sollen.

   Allgemeine Anweisungen bezüglich der Konfiguration von Mitgliedschaftsregeln finden Sie unter Verfahren zum Hinzufügen von Mitgliedschaftsregeln zu einer verwalteten Einheit weiter oben in diesem Dokument.

6. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** zu schließen.

Kopieren einer verwalteten Einheit

Mit der Quest One ActiveRoles-Konsole können Sie Kopien von verwalteten Einheiten erstellen. Mit dieser Funktion können Sie vorhandene verwaltete Einheiten wieder verwenden.

Um eine Kopie einer verwalteten Einheit zu erstellen, klicken Sie mit der rechten Maustaste auf die verwaltete Einheit und klicken Sie dann auf **Kopieren**. Hierdurch wird der Assistent „Objekt kopieren – Verwaltete Einheit" geöffnet. Sie können den Assistenten abschließen, indem Sie die Anweisungen im Abschnitt Erstellen einer verwalteten Einheit weiter oben in diesem Kapitel befolgen.

Verfahren zum Kopieren einer verwalteten Einheit

So kopieren Sie eine verwaltete Einheit:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Quest One ActiveRoles | Configuration | Managed Units**.
2. Suchen Sie unter **Managed Units** die verwaltete Einheit, die Sie kopieren möchten.
3. Klicken Sie mit der rechten Maustaste auf die verwaltete Einheit und klicken Sie dann auf **Kopieren**. Der Assistent „Objekt kopieren – Verwaltete Einheit" wird gestartet.
4. Gehen Sie auf der ersten Seite des Assistenten wie folgt vor und klicken Sie dann auf **Weiter**:
   a) Geben Sie in das Feld **Name** den Namen der verwalteten Einheit ein.
   b) Geben Sie in das Feld **Beschreibung** nach Bedarf eine Beschreibung der verwalteten Einheit ein.

5. Auf der zweiten Seite des Assistenten können Sie die Mitgliedschaftsregeln hinzufügen, entfernen und ändern, die aus der ursprünglichen verwalteten Einheit kopiert wurden. Gehen Sie wie folgt vor:
   - Um eine Mitgliedschaftsregel zur neuen verwalteten Einheit hinzuzufügen, klicken Sie auf **Hinzufügen**.
   - Um eine Mitgliedschaftsregel aus der neuen verwalteten Einheit zu entfernen, wählen Sie die Mitgliedschaftsregel aus der Liste aus und klicken Sie dann auf **Entfernen**.
   - Um eine Mitgliedschaftsregel für die neue verwaltete Einheit zu ändern, wählen Sie die Mitgliedschaftsregel aus der Liste aus und klicken Sie dann auf **Anzeigen/Bearbeiten**.

   Allgemeine Anweisungen bezüglich der Konfiguration einer Mitgliedschaftsregel finden Sie unter Verfahren zum Hinzufügen von Mitgliedschaftsregeln zu einer verwalteten Einheit weiter oben in diesem Dokument.
6. Klicken Sie auf **Weiter**.
7. Führen Sie auf der nächsten Seite des Assistenten einen der folgenden Vorgänge aus:
   - Klicken Sie auf **Sicherheit**, um Berechtigungseinstellungen für die verwaltete Einheit anzugeben.
   - Klicken Sie auf **Richtlinie**, um Richtlinieneinstellungen für die verwaltete Einheit anzugeben.

   Anweisungen bezüglich der Festlegung von Sicherheits- und Richtlinieneinstellungen finden Sie unter Verfahren zur Änderung der Berechtigungseinstellungen für eine verwaltete Einheit und Verfahren zur Änderung der Richtlinieneinstellungen für eine verwaltete Einheit weiter oben in diesem Dokument.
8. Klicken Sie auf **Weiter**.
9. Klicken Sie auf **Fertig stellen**.

Die Mitgliedschaftsregeln, Berechtigungseinstellungen und Richtlinieneinstellungen werden aus der ursprünglichen verwalteten Einheit kopiert und können dann im Assistenten „Objekt kopieren – Verwaltete Einheit" geändert werden.

Exportieren und Importieren einer verwalteten Einheit

Mit der Quest One ActiveRoles-Konsole können Sie verwaltete Einheiten in eine XML-Datei exportieren und sie dann aus dieser Datei importieren, um eine andere Instanz von Quest One ActiveRoles aufzufüllen. Die Export- und Importvorgänge stellen eine Möglichkeit bereit, verwaltete Einheiten von einer Testumgebung in eine Produktionsumgebung zu verschieben.

Wenn Sie eine verwaltete Einheit exportieren und dann importieren, werden nur Mitgliedschaftsregeln zusammen mit anderen Eigenschaften der verwalteten Einheit übertragen. Die Berechtigungs- und Richtlinieneinstellungen für die verwaltete Einheit werden nicht in den Export-Import-Vorgang eingeschlossen. Sie müssen sie nach Abschluss des Vorgangs manuell neu konfigurieren.

Um verwaltete Einheiten zu exportieren, wählen Sie sie aus, klicken Sie mit der rechten Maustaste auf die Auswahl und wählen Sie dann **Alle Aufgaben | Exportieren**. Geben Sie im Dialogfeld **Objekte exportieren** die Datei an, in der Sie die Daten speichern möchten, und klicken Sie dann auf **Speichern**.

Zum Importieren verwalteter Einheiten klicken Sie mit der rechten Maustaste auf den Container, in dem Sie die verwalteten Einheiten ablegen möchten, und klicken Sie dann auf **Importieren**. Wählen Sie im Dialogfeld **Verzeichnisobjekte importieren** die Datei aus, in die die verwalteten Einheiten exportiert wurden, und klicken Sie dann auf **Öffnen**.

Umbenennen einer verwalteten Einheit

Um eine verwaltete Einheit umzubenennen, klicken Sie mit der rechten Maustaste auf die verwaltete Einheit und klicken dann auf **Umbenennen**. Geben Sie den neuen Namen ein und drücken Sie dann die Eingabetaste.

Das Umbenennen einer verwalteten Einheit hat keine Auswirkungen auf die Mitgliedschaftsregeln, Berechtigungseinstellungen oder Richtlinieneinstellungen, die der verwalteten Einheit zugeordnet sind.

Verfahren zum Umbenennen einer verwalteten Einheit

So benennen Sie eine verwaltete Einheit um:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Quest One ActiveRoles | Configuration | Managed Units**.
2. Suchen Sie unter **Managed Units** die verwaltete Einheit, die Sie umbenennen möchten, klicken Sie mit der rechten Maustaste darauf und klicken Sie dann auf **Umbenennen**.
3. Geben Sie einen neuen Namen ein und drücken Sie dann die Eingabetaste.

Löschen einer verwalteten Einheit

Um eine verwaltete Einheit zu löschen, klicken Sie mit der rechten Maustaste auf die verwaltete Einheit und klicken dann auf **Löschen**.

Wenn Sie eine verwaltete Einheit löschen, werden die darin enthaltenen Objekte nicht gelöscht. Der Löschvorgang löscht die Mitgliedschaftsregeln, Berechtigungseinstellungen und Richtlinieneinstellungen, die der verwalteten Einheit zugeordnet sind.

Verfahren zum Löschen einer verwalteten Einheit

So löschen Sie eine verwaltete Einheit:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Quest One ActiveRoles | Configuration | Managed Units**.
2. Suchen Sie unter **Managed Units** die verwaltete Einheit, die Sie löschen möchten, klicken Sie mit der rechten Maustaste darauf und klicken Sie dann auf **Löschen**.

Wenn Sie eine verwaltete Einheit löschen, werden deren Mitglieder nicht gelöscht. Die Berechtigungseinstellungen und die Richtlinieneinstellungen, die über die verwaltete Einheit festgelegt wurden, sind jedoch nicht mehr gültig, wenn die verwaltete Einheit gelöscht wurde.

Szenario: Implementieren der rollenbasierten Verwaltung über mehrere Organisationseinheiten hinweg

In diesem Szenario wird eine administrative Ansicht mit dem Namen **Vertrieb** erstellt. Sie befindet sich in einer Organisation mit der Active Directory-Struktur, die auf Organisationseinheiten basiert.

Angenommen, eine Organisation verfügt über Niederlassungen in den USA und Kanada. Die Regel für das Einschließen eines Benutzers in eine Organisationseinheit ist der geografische Standort des Benutzers. Daher befinden sich alle Benutzer, die in den USA arbeiten, in der Organisationseinheit **USA**, und die, die in Kanada arbeiten, befinden sich in der Organisationseinheit **Kanada**.

Die Büros in den USA und in Kanada haben jeweils eine **Marketing**-, **Entwicklungs**- und **Vertriebsabteilung**. Indem Sie die verwaltete Einheit **Vertrieb** erstellen, können Sie Benutzer aus den **Vertriebsabteilungen** in den USA und Kanada gemeinsam verwalten, ohne die eigentliche, auf Organisationseinheiten basierende Struktur zu ändern.

Beim Delegieren der Kontrolle über eine verwaltete Einheit erben alle Benutzer in dieser verwalteten Einheit Sicherheitseinstellungen, die auf der Ebene der verwalteten Einheit definiert sind. Daher werden beim Anwenden einer Zugriffsvorlage auf eine verwaltete Einheit die Sicherheitseinstellungen für jeden Benutzer in der verwalteten Einheit festgelegt.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen Sie die verwaltete Einheit **Sales**.
2. Fügen Sie Benutzer aus den **Vertriebsabteilungen** in den USA und Kanada zur verwalteten Einheit **Sales** hinzu.
3. Bereiten Sie die Zugriffsvorlage **Sales** vor.
4. Wenden Sie die Zugriffsvorlage **Sales** auf die verwaltete Einheit **Vertrieb** an und wählen Sie eine geeignete Gruppe als Trustee aus.

Folglich erhalten die Mitglieder der Gruppe Kontrolle über Benutzerkonten, die der verwalteten Einheit **Vertrieb** angehören. Der Bereich der Kontrolle wird durch die Berechtigungen in der Zugriffsvorlage **Sales** definiert.

In den folgenden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen der verwalteten Einheit

Im ersten Schritt erstellen Sie die verwaltete Einheit **Vertrieb**. Informationen bezüglich der Erstellung einer verwalteten Einheit finden Sie unter Erstellen einer verwalteten Einheit weiter oben in diesem Kapitel.

Schritt 2: Hinzufügen von Benutzern zu der verwalteten Einheit

Nach dem Vorbereiten der verwalteten Einheit **Vertrieb** fügen Sie ihre Benutzer aus den **Vertriebsabteilungen** im gesamten Unternehmen hinzu.

Nehmen Sie an, dass für alle Benutzer in den **Vertriebsabteilungen** (in den USA und in Kanada) die Eigenschaft **Beschreibung** auf **Sales** festgelegt ist.

Erstellen Sie eine Mitgliedschaftsregel vom Typ **Nach Abfrage einschließen** mit folgenden Parametern: Wählen Sie aus der Liste **Suchen** die Option **Benutzer** aus. Geben Sie in das Feld **Beschreibung** den Wert **Vertrieb** ein. Somit werden alle Benutzer mit der Beschreibung **Vertrieb** in die verwaltete Einheit eingeschlossen.

Weitere Informationen bezüglich der Erstellung von Mitgliedschaftsregeln finden Sie unter Hinzufügen und Entfernen von Mitgliedern einer verwalteten Einheit weiter oben in diesem Kapitel.

Schritt 3: Vorbereiten der Zugriffsvorlage

Um die Rechte des Trustees für die verwaltete Einheit **Vertrieb** zu definieren, erstellen Sie die Zugriffsvorlage **Sales** und fügen Sie ihr Berechtigungen hinzu.

Weitere Informationen bezüglich der Erstellung einer Zugriffsvorlage finden Sie unter Erstellen einer Zugriffsvorlage weiter unten in diesem Dokument.

Schritt 4: Anwenden der Zugriffsvorlage

Um die Zugriffsvorlage **Sales** auf die verwaltete Einheit **Vertrieb** anzuwenden, klicken Sie mit der rechten Maustaste auf die verwaltete Einheit **Sales** und klicken Sie auf **Kontrolle delegieren**. Klicken Sie dann auf die Schaltfläche **Hinzufügen** und befolgen Sie die Anleitungen im Assistenten zum Delegieren der Kontrolle.

Fügen Sie auf der Seite **Benutzer oder Gruppen** des Assistenten den Benutzer oder die Gruppe hinzu, der bzw. die als Trustee ausgewählt werden sollen.

Wählen Sie auf der Seite **Zugriffsvorlagen** des Assistenten die Zugriffsvorlage **Sales** aus, die Sie in Schritt 3 vorbereitet haben.

Weitere Informationen über die Anwendung einer Zugriffsvorlage auf eine verwaltete Einheit finden Sie unter Anwenden von Zugriffsvorlagen weiter unten in diesem Dokument.

Überlegungen bezüglich der Bereitstellung

Verwaltete Einheiten können am besten als virtuelle Organisationseinheiten beschrieben werden, die es Ihnen ermöglichen, von der Delegation und Richtlinienanwendung innerhalb einer logischen Gruppierung von Objekten zu profitieren, die nicht immer mit Ihrer Active Directory-Struktur übereinstimmen muss. In ihrer gröbsten Form sind verwaltete Einheiten nichts mehr als in der Konfigurationsdatenbank von Quest One ActiveRoles gespeicherte LDAP-Abfragen. Als solche können verwaltete Einheiten nur über die Benutzeroberflächen von Quest One ActiveRoles aufgerufen und konfiguriert werden. Dieser Abschnitt deckt die folgenden Themen ab, um Sie bei der bestmöglichen Nutzung von verwalteten Einheiten zu unterstützen:

- Mitgliedschaftsregeln für die verwaltete Einheit
- Delegieren von verwalteten Einheiten

Mitgliedschaftsregeln für die verwaltete Einheit

Mitgliedschaftsregeln bestimmen die Liste der in eine verwaltete Einheit aufzunehmenden Objekte fest. Obwohl verschiedene Arten von Mitgliedschaftsregeln verfügbar sind, werden üblicherweise zwei Arten verwendet. Hierbei handelt es sich um abfragebasierte Aufnahme- bzw. Ausschlussregeln und explizite Aufnahme- bzw. Ausschlussregeln.

Normalerweise verwenden Sie abfragebasierte Regeln, um Objekte aufzunehmen, die mehrere Organisationseinheiten oder Organisationseinheit-Strukturen umspannen. Ein Beispiel hierfür ist eine verwaltete Einheit, die alle deaktivierten Benutzerkonten umfasst, oder eine verwaltete Einheit, die alle Benutzerkonten ohne Postfächer umfasst. Abfragebasierte Regeln werden auch verwendet, um logische Strukturen auf der Grundlage einer flachen Organisationseinheit-Struktur zu erstellen.

Gehen Sie bei der Verwendung von abfragebasierten Regeln sorgfältig vor, weil es sich hierbei im Wesentlichen um Bedingungen handelt, die Objektattributen auferlegt werden. Wenn der Wert des Attributs eines Objekts nicht den angegebenen Bedingungen entspricht, wird das Objekt nicht in die verwaltete Einheit aufgenommen. Das Gegenteil gilt ebenfalls. Wenn Sie beispielsweise eine verwaltete Einheit so konfigurieren, dass sie alle Benutzer enthalten soll, deren Name mit dem Buchstaben A beginnt, so würde die verwaltete Einheit aus das Administratorkonto enthalten. Wenn die Kontrolle über diese verwaltete Einheit an das Help Desk delegiert ist, so könnten die Operatoren des Help Desk Kontrolle über das Administratorkonto erlangen. Aus diesem Grund ist die Verwendung expliziter Regeln erforderlich.

Explizite Regeln ermöglichen Ihnen, Objekte auf der Grundlage Ihrer Kennung (GUID) aufzunehmen bzw. auszuschließen. Unabhängig davon, ob das Objekt geändert oder umbenannt wird: die Regel gilt, solange das Objekt im Verzeichnis vorhanden ist. Explizite Regeln ergänzen normalerweise die abfragebasierten Regeln, um ein Objekt aufzunehmen, das von der Abfrage nicht abgedeckt wird, oder um ein Objekt auszuschließen, dass die Bedingungen der Abfrage möglicherweise erfüllt. Zu den weiteren Verwendungen zählt die statische Aufnahme eines Objekts, so dass dieses Objekt unabhängig von dessen Benennung immer aufgenommen wird. Üblicherweise handelt es sich hierbei um Organisationseinheiten. Sie können eine logische Struktur von Organisationseinheiten aus jedem Teil der Verzeichnisstruktur erstellen, indem Sie sie explizit zu einer verwalteten Einheit hinzufügen. Dies erleichtert die Delegation und Richtlinienanwendung in erheblichem Maß, da Beides auf der Ebene der verwalteten Einheit anstelle auf der Ebene jeder einzelnen Organisationseinheit durchgeführt werden kann.

In der folgenden Tabelle sind einige nützliche Beispiele für Mitgliedschaftsregeln aufgeführt. Diese Beispiele zeigen, wie die Mitgliedschaftsregeln mittels LDAP-Filter kontrolliert werden können. Sie können einen LDAP-Filter unter der Option **Benutzerdefinierte Suche** in einem der abfragebasierten Regeltypen anwenden.

INHALT DER VERWALTETEN EINHEIT	LDAP-FILTER
In der Exchange-Adressliste ausgeblendete Gruppen	(&(objectCategory=group)(mailnickName=*)(msExchHideFromAddressLists=True))
Mail-aktivierte Gruppen	(&(objectCategory=group)(mailNickName=*))
Mail-aktivierte Benutzer mit festgelegter Weiterleitung	(&(sAMAccountType=805306368)(mailNickName=*)(altRecipient=*))
Benutzer, die über kein Exchange-Postfach verfügen	(&(sAMAccountType=805306368)(!(homeMDB=*)))

INHALT DER VERWALTETEN EINHEIT	LDAP-FILTER
Verteilergruppen	(&(objectCategory=group)(!(groupType:1.2.840.113556.1.4.803:=2147483648)))
Sicherheitsgruppen	(&(objectCategory=group)(groupType:1.2.840.113556.1.4.803:=2147483648))
Deaktivierte Benutzerkonten	(&(objectCategory=user)(userAccountControl:1.2.840.113556.1.4.803:=2))
Benutzer aus der Sales-Abteilung	(&(objectCategory=user)(department=Sales))

Delegieren von verwalteten Einheiten

Sie können verwaltete Einheiten genau so wie Organisationseinheiten oder eine gesamte Domäne delegieren, indem Sie Zugriffsvorlagen in Quest One ActiveRoles anwenden. Dies kann die Bereitstellung in erheblichem Maß beschleunigen, die administrative Last für Quest One ActiveRoles selbst reduzieren und die Schulungs- und Arbeitsverfahren für die Administratoren, die dieses Tool verwenden, erleichtern.

Sie können beispielsweise durch die Gruppierung aller deaktivierten und gesperrten Konten innerhalb einer einzelnen verwalteten Einheit die Kontrolle an eine Help Desk-Gruppe delegieren, so dass diese schnell und einfach einen Großteil ihrer Jobfunktion durchführen können, indem sie nur eine einzelne Struktur aufzählen und durchgucken müssen. Außerdem müssen Sie, wenn Sie die Kontrolle über eine verwaltete Einheit delegieren, Ihren delegierten Administratoren keinen Zugriff auf irgendeine Organisationseinheit selbst gewähren; alle Objekte, die den Mitgliedschaftsregeln entsprechen, befinden sich unabhängig davon, welche Organisationseinheiten diese Objekte enthalten, in der verwalteten Gruppe.

Ein weiteres Beispiel wäre, wenn Active Directory über eine sehr flache Struktur an Organisationseinheiten verfügt, jedoch verschiedene Administratoren für verschiedene Standorte verantwortlich sind. So lande der Standortcode in einem Attribut der zu verwaltenden Objekte gespeichert ist, können Sie verwaltete Einheiten auf der Basis dieses Attributs erstellen und jeder Administratorengruppe eine verwaltete Einheit zuweisen, die deren entsprechende Objekte enthält, die einem bestimmten Standortcode entsprechen. Da verwaltete Einheiten eine reine Gruppierung von Objekten auf der Grundlage bestimmter Attribute sind, bewegen sich die Objekte unabhängig davon, wie sich deren Objekte ändern, entweder über die Benutzeroberflächen von Quest One ActiveRoles oder nativ in bzw. aus den verwalteten Einheiten.

Eine wichtige Funktion der verwalteten Einheiten ist die Tatsache, dass eine einzige verwaltete Einheit Objekte aus jeder beliebigen, von Quest One ActiveRoles verwalteten Domäne (verwaltete Domänen) enthalten kann. So lange eine bestimmte Domäne bei Quest One ActiveRoles registriert ist, kann jedes beliebige Objekt aus dieser Domäne unabhängig von der Gesamtstruktur der Domäne zu einer verwalteten Einheit hinzugefügt werden. Beim Delegieren einer verwalteten Einheit, die Objekte aus verschiedenen Domänen enthält, empfiehlt es sich, domänenspezifische Gruppen aus der Domäne, in der sich die Quest One ActiveRoles-Installation befindet, oder universelle Gruppen zu verwenden. Der Grund ist, dass Quest One ActiveRoles Ihnen die Delegation zu jeder Sicherheitsgruppe innerhalb der verwalteten Domänen ermöglicht; wenn jedoch die Quest One ActiveRoles-Installation in Domäne A existiert und eine Delegation zu einer domänenspezifischen Gruppe in Domäne B erfolgt ist, so wird einem Administrator, der sich bei Quest One ActiveRoles in Domäne A authentifiziert, niemals die lokale Gruppe aus Domäne B zu seinem Sicherheits-Token hinzugefügt, und aus diesem Grund wird er nicht über seine delegierten Rechte verfügen. Außerdem können globale Gruppen verwendet werden, solange sich alle administrativen Benutzer in der Domäne befinden, in der Quest One ActiveRoles installiert ist.

Beim Delegieren der Kontrolle über verwaltete Einheiten muss die Möglichkeit zur Synchronisation der delegierten Berechtigungen mit Active Directory berücksichtigt werden. Wenn Sie eine Zugriffsvorlage auf eine verwaltete Einheit anwenden und die Berechtigungen nicht mit Active Directory synchronisieren, werden die Berechtigungseinstellungen nur in der Konfigurationsdatenbank von Quest One ActiveRoles gespeichert. Quest One ActiveRoles behält die Eltern/Kind-Beziehung für die in der verwaltete Einheit enthaltenen Objekte bei und ermöglicht somit die Vererbung der Berechtigungen. Wenn Sie wählen, die Berechtigungen mit Active Directory zu synchronisieren, gibt es keine Möglichkeit, die Eltern/Kind-Beziehung in Active Directory beizubehalten, da eine verwaltete Einheit kein echtes Objekt innerhalb von Active Directory ist. Für Active Directory existiert dieses übergeordnete Objekt nicht. Folglich wird jeder in der Zugriffsvorlage gefundene Berechtigungseintrag in die native Zugriffskontrollliste jedes in der verwalteten Einheit enthaltenen Objekts aufgenommen. Dies kann potenziell zu Leistungseinbußen führen.

4

Rollenbasierte Administration

- Zugriffsvorlagen zum Definieren von Administratorfunktionen
- Verwaltungsaufgaben für Zugriffsvorlagen
- Verwendungsbeispiele
- Überlegungen bezüglich der Bereitstellung

Zugriffsvorlagen zum Definieren von Administratorfunktionen

Quest One ActiveRoles gewährleistet eine sichere, dezentrale Verwaltung durch die erweiterte Übertragung von Rechten mit sehr hoher Granularität auf einzelne Benutzer oder Gruppen. Dies nimmt hoch qualifizierten Administratoren tägliche Routineaufgaben ab und spart ihnen Zeit, sodass ihre Produktivität erhöht wird. Beispielsweise kann ein Administrator dem Help Desk die Ausführung bestimmter Aufgaben (z.B. das Zurücksetzen von Kennwörtern oder das Verwalten von Gruppenmitgliedschaften) gestatten, ohne den Help Deskmitarbeitern vollständige Administratorrechte zu erteilen.

Beim Entwickeln des Verwaltungs- und Sicherheitsentwurfs definieren Sie delegierte Administratoren (Trustees) sowie Administratorfunktionen (Zugriffsvorlagen). Dann definieren Sie verwaltete Einheiten und wenden Zugriffsvorlagen an, wobei Sie für jede verwaltete Einheit Trustees auswählen. Sie können Zugriffsvorlagen auch auf Objekte und Ordner in Active Directory anwenden und so die Berechtigungen den erforderlichen Trustees zuweisen. Diese dreiseitige Beziehung zwischen Trustees, Zugriffsvorlagen und verwalteten Objekten ist für die Implementierung Ihres rollenbasierten Verwaltungsmodells zentral.

Das Tool „Benutzer und Computer" von Active Directory ermöglicht die Delegierung von Administrator-Verantwortlichkeiten. aber bei jeder Delegierung von Rechten müssen auch eine Reihe von Berechtigungen definiert werden. Dadurch wird der Delegierungsvorgang zeitaufwändig und fehleranfällig. Quest One ActiveRoles überwindet dieses Problem durch die Bundelung von Berechtigungen in individuell anpassbaren Gruppen von Verwaltungsrechten den Zugriffsvorlagen. Die logische Gruppierung von Berechtigungen vereinfacht die Verwaltung von Delegierungseinstellungen.

Zugriffsvorlagen sind Sammlungen von Berechtigungen, die Administratorfunktionen darstellen. Berechtigungen werden verwendet, um einem Benutzer oder einer Gruppe bestimmte administrative Vorgänge zu gestatten oder zu verbieten. Sie können eine Zugriffsvorlage erstellen, die alle erforderlichen Berechtigungen für die Ausführung einer bestimmten Administratorfunktion enthalten.

Um einem Benutzer oder einer Gruppe die Funktion zuzuweisen, sollten Sie die Zugriffsvorlage je nach dem Gültigkeitsbereich der Funktion mit einer verwalteten Einheit, einer Organisationseinheit, einer Domäne oder einem einzelnen Objekt verknüpfen und dann einen Benutzer oder eine Gruppe als Trustee auswählen. Infolgedessen erhält der einzelne Benutzer bzw. jedes Mitglied der Gruppe die durch die Funktion angegebenen Rechte zum Verwalten von Objekten in der Auflistung oder dem Ordner, mit der bzw. dem die Zugriffsvorlage verknüpft wurde.

Funktionsweise von Zugriffsvorlagen

Quest One ActiveRoles setzt die delegierte Verwaltung durch die Verknüpfung von Zugriffsvorlagen mit Objektsammlungen (verwalteten Einheiten), Verzeichnisordnern (Containern) oder einzelnen (Blatt-) Objekten um.

Bei Anwendung auf ein Verzeichnisobjekt gibt eine Zugriffsvorlage Berechtigungseinstellungen für dieses Objekt und seine untergeordneten Objekte an. Durch Anwenden von Zugriffsvorlagen auf verwaltete Einheiten können Berechtigungen für Auflistungen von Verzeichnisobjekten bequem verwaltet werden.

Jede Zugriffsvorlage wird in Bezug auf einige Benutzer und/oder Gruppen (Trustees) angewendet, und die in der Zugriffsvorlage festgelegten Berechtigungen bestimmen ihren Zugriff auf verwaltete Objekte. Wenn eine Zugriffsvorlage verändert oder nicht mehr angewendet wird, werden die für die Verzeichnisobjekte festgelegten Berechtigungen entsprechend geändert.

Bei einer Änderung der Berechtigungen für eine verwaltete Einheit berechnet Quest One ActiveRoles die Berechtigungseinstellungen für alle Mitglieder der verwalteten Einheit neu. Ebenso werden die Berechtigungsinformationen geändert, wenn die Liste der Objekte in einer verwalteten Einheit geändert wird. Wenn Objekte der verwalteten Einheit hinzugefügt oder aus ihr entfernt werden (beispielsweise aufgrund von Änderungen an Objekteigenschaften), werden alle Berechtigungseinstellungen für diese Objekte neu berechnet.

Jedes Objekt erbt seine Berechtigungseinstellungen von den verwalteten Einheiten, in denen es sich befindet. Wenn ein Trustee beispielsweise über Zugriffsberechtigungen für mehrere verwaltete Einheiten verfügt, die ein bestimmtes Objekt enthalten, sind die Zugriffsberechtigungen des Trustees für dieses Objekt einfach als Vereinigung aller Berechtigungen definiert, die auf der Ebene der verwalteten Einheiten angegeben sind.

Bei der Anwendung von Zugriffsvorlagen auf ein Containerobjekt (einen Verzeichnisordner) wird der Zugriff des Trustees auf den Container und seine untergeordneten Objekte eingerichtet. Durch die angegebenen Berechtigungen für einen Container verfügt der Trustee auch über vererbte Berechtigungen für die untergeordneten Objekte in dem Container.

Sicherheitssynchronisierung

Die in einer Zugriffsvorlage festgelegten Berechtigungen können an Active Directory weitergereicht werden, wobei alle in Quest One ActiveRoles an ihnen vorgenommenen Änderungen automatisch mit Active Directory synchronisiert werden.

Durch Einschalten der Synchronisierung der Sicherheit von Quest One ActiveRoles mit der internen Sicherheit von Active Directory bietet Quest One ActiveRoles die Möglichkeit, die Sicherheitseinstellungen von Active Directory mithilfe von Zugriffsvorlagen festzulegen. Zugriffsvorlagen vereinfachen und erweitern die Verwaltung von Berechtigungen in Active Directory, ermöglichen die logische Gruppierung von Berechtigungen und stellen einen effizienten Mechanismus für das Festlegen und Aufrechterhalten der Zugriffskontrolle dar.

Für jeden in Quest One ActiveRoles festgelegten und mit der Auswahl der Möglichkeiten zur **Weitergabe der Berechtigungen** eingerichteten Berechtigungseintrag legt Quest One ActiveRoles auf der Grundlage des jeweiligen Quest One ActiveRoles-Berechtigungseintrags einen entsprechenden internen Berechtigungseintrag in Active Directory an.

Durch Einschalten der Möglichkeit der **Weitergabe der Berechtigungen** (auf der Arbeitsoberfläche auch als **Mit interner Sicherheit synchronisieren** oder **Mit AD synchronisieren** bezeichnet) ist gewährleistet, dass die verknüpften internen Sicherheitseintrage bei jeder Änderung der Berechtigungen in Quest One ActiveRoles entsprechend geändert werden.

Durch das Abschalten der Auswahlmöglichkeit zur **Weitergabe der Berechtigungen** bei bestehenden Quest One ActiveRoles-Berechtigungen oder das Löschen von Quest One ActiveRoles-Berechtigungen mithilfe der hier gegebenen Auswahlmöglichkeiten werden alle durch diese Quest One ActiveRoles-Berechtigungen festgelegten internen Berechtigungseintrage gelöscht.

Wird ein weitergegebener Berechtigungseintrag in Active Directory absichtlich oder versehentlich gelöscht oder geändert, so stelltQuest One ActiveRoles diesen Eintrag anhand der Angaben in der Zugriffsvorlage wieder her, wodurch die zutreffenden Berechtigungseinstellungen in Active Directory sichergestellt sind. In Quest One ActiveRoles wird der planmäßige Vorgang der „Synchronisierung der Berechtigungen mit Active Directory" dazu verwendet, Berechtigungseintrage in Active Directory auf der Grundlage der Zugriffsvorlagenverknupfungen mit eingeschalteter Berechtigungsweitergabe anzulegen oder zu aktualisieren.

Verwaltungsaufgaben für Zugriffsvorlagen

In diesem Abschnitt wird die Verwaltung der Zugriffsvorlagen mithilfe der Programmsteuerung von Quest One ActiveRoles vorgestellt. Folgende Themen werden erörtert:

- Verwenden vordefinierter Zugriffsvorlagen
- Erstellen einer Zugriffsvorlage
- Anwenden von Zugriffsvorlagen
- Verwalten von Zugriffsvorlagenverknüpfungen
- Synchronisieren von Berechtigungen mit Active Directory
- Hinzufügen, Ändern und Entfernen von Berechtigungen
- Schachteln von Zugriffsvorlagen
- Kopieren einer Zugriffsvorlage
- Exportieren und Importieren von Zugriffsvorlagen
- Umbenennen einer Zugriffsvorlage
- Löschen einer Zugriffsvorlage

Verwenden vordefinierter Zugriffsvorlagen

Quest One ActiveRoles bietet eine umfangreiche Sammlung vorkonfigurierter Access-Vorlagen, die typische Verwaltungsrollen darstellen, welche die rasche und konsistente Delegierung der korrekten Ebene der Verwaltungsautorität ermöglichen.

Die vorgefertigten Zugriffsvorlagen finden sich in Containerverzeichnissen unter **Einrichtungseinstellungen / Zugriffsvorlagen** in der Quest One ActiveRoles-Programmsteuerung. Sie können im Bereich „Details" eine Liste von Zugriffsvorlagen anzeigen, indem Sie **Configuration | Access Templates** erweitern und einen der folgenden Container in der Konsolenstruktur auswählen:

- Active Directory
- AD LDS (ADAM)
- Computerressourcen
- Konfiguration
- Exchange
- Benutzer-Selbstverwaltung

Active Directory

Sie können Zugriffsvorlagen aus dem Container **Active Directory** verwenden, um Datenverwaltungsaufgaben von Active Directory und Dienstverwaltungsaufgaben von Active Directory zu delegieren, z.B:

- Benutzer- und Gruppenverwaltung
- Verwaltung von Objekten für Computer, Druckerwarteschlangen oder freigegebene Ordner
- Verwaltung der Gesamtstruktur- und Domänenkonfiguration

Dieser Container enthält Vorlagen für zahlreiche Verwaltungsaufgaben und Vorlagen, die den Zugriff auf ausgewählte Eigenschaften von Active Directory-Objekten einschränken.

AD LDS (ADAM)

Die Zugriffsvorlagen aus dem Container **AD LDS (ADAM)** können zur Delegierung von Datenverwaltungsaufgaben in Bezug auf die folgenden Objektarten der Lightweight-Verzeichnisdienste in Active Directory (AD LDS) verwendet werden:

- AD LDS-Container
- AD LDS-Gruppe
- AD LDS-Organisationseinheit
- AD LDS-Benutzer

Anweisungen bezüglich der Anzeige oder der Festlegung von Berechtigungen für AD LDS-Objekte finden Sie im Kapitel „AD LDS-Datenverwaltung" weiter unten in diesem Dokument.

Computerressourcen

Mit Zugriffsvorlagen aus dem Container **Computer Resources** können Sie Verwaltungsaufgaben für Ressourcen delegieren, die sich auf lokalen Computern befinden, z.B.:

- Lokale Benutzer und Gruppen
- Dienste
- Netzwerkdateifreigaben (freigegebene Verzeichnisse)
- Drucker und Druckaufträge

Dieser Container enthält Vorlagen für bestimmte Administratorfunktionen (z.B. den Druckeroperator oder den Dienstoperator), sowie Vorlagen, mit denen der Zugriff auf ausgewählte Eigenschaften lokaler Computerressourcen angegeben wird.

Konfiguration

Zugriffsvorlagen aus dem Container für die **Einrichtungseinstellungen** sind zur Delegierung von Datenverwaltungsaufgaben in Bezug auf die Einrichtungseinstellungen von Quest One ActiveRoles verwendbar, beispielsweise:

- Administration verwalteter Einheiten, Richtlinienobjekte oder Zugriffsvorlagen
- Konfigurieren der Replikation (Hinzufügen oder Entfernen von Replikationspartnern)
- Hinzufügen oder Entfernen verwalteter Domänen

Dieser Container schließt auch Vorlagen ein, die den Zugriff auf einzelne Eigenschaften von verwalteten Einheiten, Richtlinienobjekten und Zugriffsvorlagen steuern.

Exchange

Mit Zugriffsvorlagen aus dem Container **Exchange** können Sie die folgenden Verwaltungsaufgaben für Exchange Server-Empfänger delegieren:

- Verwaltung aller Empfängereinstellungen
- Assistent für Exchange-Aufgaben verwenden
- Verwaltung von E-Mail-Adressen
- Konfigurieren allgemeiner Nachrichteneinstellungen
- Konfigurieren erweiterter Nachrichteneinstellungen

Dieser Container enthält außerdem Vorlagen, die den Zugriff auf einzelne, auf Exchange bezogene Eigenschaften von Benutzern, Gruppen und Kontakten steuern.

Benutzer-Selbstverwaltung

Zugriffsvorlagen aus dem Container **Vom Benutzer selbst verwaltet** werden verwendet, um Selbstverwaltungsaufgaben an Endbenutzer zu delegieren (zum Beispiel die Berechtigung der Benutzer, mithilfe der Selbstverwaltungs-Web-Schnittstelle von Quest One ActiveRoles Änderungen an ihren eigenen Konten vorzunehmen).

Um eine Zugriffsvorlage detailliert zu untersuchen, zeigen Sie das Dialogfeld **Eigenschaften** wie folgt an: Klicken Sie mit der rechten Maustaste auf Zugriffsvorlage und klicken Sie dann auf **Eigenschaften**. Auf der Registerkarte **Berechtigungen** im Dialogfeld **Eigenschaften** werden alle in der Zugriffsvorlage definierten Berechtigungseinträge aufgelistet. Sie können jeden Eintrag wie folgt untersuchen: Wählen Sie einen Eintrag aus und klicken Sie auf die Schaltfläche **Anzeigen**.

Quest One ActiveRoles gestattet weder die Änderung noch das Loschen vorgefertigter Zugriffsvorlagen. Wenn Sie Änderungen an einer vordefinierten Zugriffsvorlage vornehmen möchten, müssen Sie eine Kopie der Zugriffsvorlage erstellen und diese nach Bedarf verändern. Zum Erstellen einer Kopie klicken Sie mit der rechten Maustaste auf die Zugriffsvorlage und dann auf **Kopieren**.

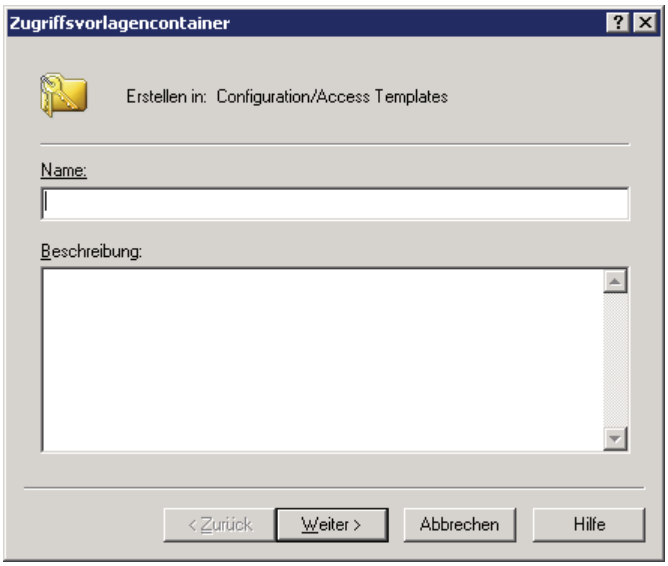
Sie können eine Zugriffsvorlage anwenden, indem Sie den Assistenten Delegation der Kontrolle verwenden: Klicken Sie mit der rechten Maustaste auf die Zugriffsvorlage, klicken Sie auf **Verknüpfungen** und klicken Sie dann im Fenster **Verknüpfungen** auf **Hinzufügen**, um den Assistenten zu starten. Ausführlichere Informationen finden Sie unter Anwenden von Zugriffsvorlagen weiter unten in diesem Kapitel.

Erstellen einer Zugriffsvorlage

Die Programmsteuerung von Quest One ActiveRoles halt zum Anlegen von Zugriffsvorlagen den Assistenten „Neues Objekt - Zugriffsvorlage" bereit. Sie können den Assistenten auf folgende Weise starten: Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Access Templates** und wählen Sie **Neu | Zugriffsvorlage** aus. In diesem Fall fügt der Assistent eine Zugriffsvorlage zum Container **Access Templates** hinzu.

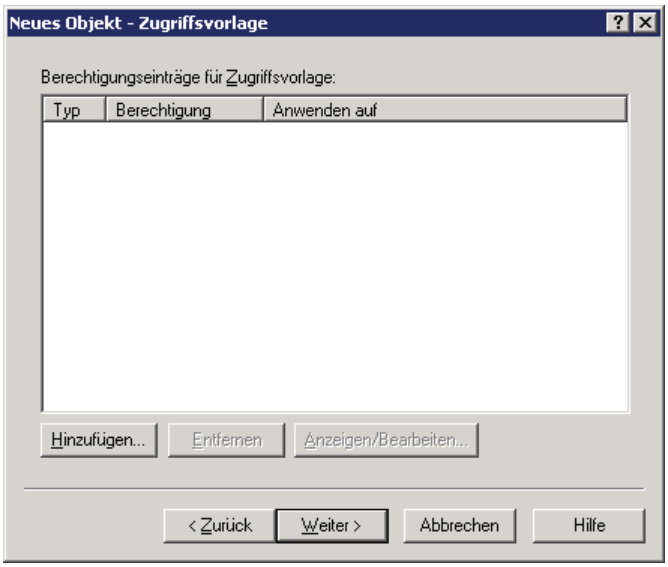
Sie sollten benutzerdefinierte Zugriffsvorlagen in einem separaten Container speichern. Sie können wie folgt einen Container erstellen: Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Access Templates** und wählen Sie **Neu | Zugriffsvorlagencontainer** aus. Nachdem Sie einen Container erstellt haben, können Sie mit Hilfe des Assistenten eine Zugriffsvorlage zu dem Container anstatt direkt zu den **Access Templates** hinzufügen: Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Container und wählen Sie **Neu | Zugriffsvorlage** aus.

Die erste Seite des Assistenten entspricht der folgenden Abbildung.



Geben Sie auf dieser Seite einen Namen und eine Beschreibung für die neue Zugriffsvorlage ein. In der Quest One ActiveRoles-Programmsteuerung werden im Angabenfenster in der Zugriffsvorlagenaufstellung der Name und die Beschreibung angezeigt.

Klicken Sie auf **Weiter**. Die zweite Seite des Assistenten ähnelt der folgenden Abbildung.

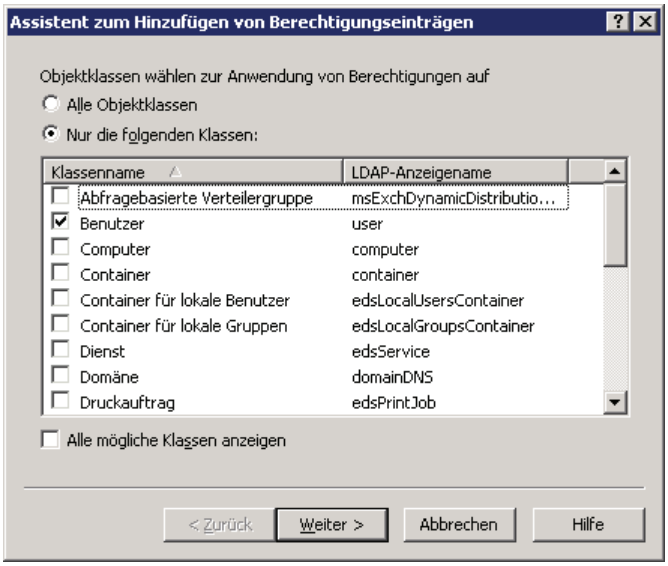


Auf dieser Seite werden Sie aufgefordert, eine Liste von Berechtigungseinträgen für Zugriffsvorlagen zu konfigurieren. Mit den Schaltflächen **Hinzufügen**, **Entfernen** und **Anzeigen/Bearbeiten** können Sie einen Eintrag hinzufügen, entfernen bzw. ändern. Durch Anklicken von **Hinzufügen** wird der Assistent zum Hinzufügen von Berechtigungseinträgen gestartet, der Sie bei der Konfiguration der Berechtigungseinträge unterstützt. Der Assistent wird weiter unten in diesem Abschnitt beschrieben.

Nachdem Sie die Liste der Berechtigungseinträge abgeschlossen haben, klicken Sie auf **Weiter** und dann auf **Fertig stellen**. Die neue Zugriffsvorlage wird erstellt.

Assistent zum Hinzufügen von Berechtigungseinträgen

Der Assistent zum Hinzufügen von Berechtigungseinträgen ermöglicht Ihnen die Festlegung der Berechtigungen, die zur Zugriffsvorlage hinzugefügt werden sollen. Die erste Seite des Assistenten entspricht der folgenden Abbildung.

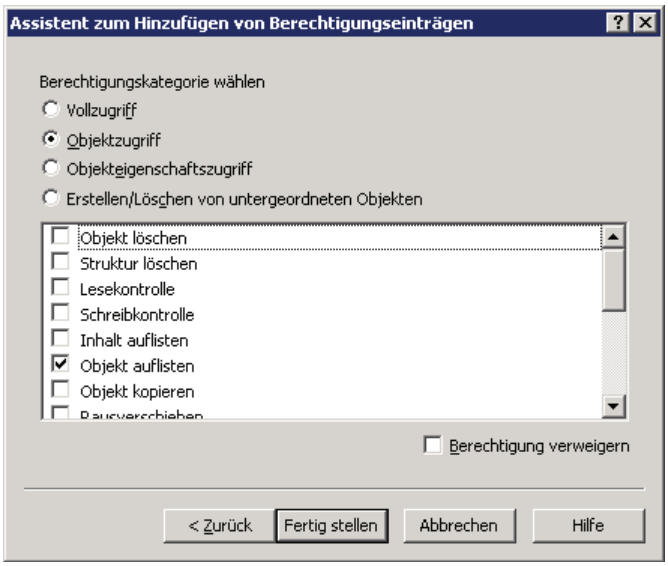


Auf dieser Seite wählen Sie die Typen von Objekten aus, denen Sie mit dieser Berechtigung den Zugriff gewähren (oder verweigern) möchten. Sie können eine der folgenden Optionen auswählen:

- **Alle Objektklassen.** Mit dieser Option steuert die Berechtigung den Zugriff auf Objekte beliebigen Typs.
- **Nur die folgenden Klassen.** Mit dieser Option steuert die Berechtigung den Zugriff auf Objekte des Typs, den Sie auswählen, indem Sie die entsprechenden Kontrollkästchen in der Liste aktivieren.

Standardmäßig werden nicht alle Objektklassen in der Liste angezeigt. Um alle Objektklassen anzuzeigen, aktivieren Sie das Kontrollkästchen **Alle mögliche Klassen anzeigen**.

Klicken Sie nach dem Auswählen der gewünschten Objektklassen auf **Weiter**. Die nächste Seite des Assistenten entspricht der folgenden Abbildung.



Auf dieser Seite wählen Sie eine Berechtigungskategorie aus und geben an, ob die Berechtigung bestimmte administrative Aktionen zulassen oder verweigern soll.

Sie können eine der folgenden Berechtigungskategorien auswählen:

- **Vollzugriff.** Lässt alle administrativen Aktionen für ein Objekt zu oder verweigert sie.
- **Objektzugriff.** Steuert, wie auf ein Objekt zugegriffen und wie es kontrolliert wird.
- **Objekteigenschaftszugriff.** Steuert den Zugriff auf die Attribute eines Objekts.
- **Erstellen/Löschen von untergeordneten Objekten.** Gewährt oder verweigert die Erstellung oder Löschung von Objekten in einem Container.

Wenn die Berechtigung bestimmte administrative Aktionen verweigern soll, aktivieren Sie das Kontrollkästchen **Berechtigung verweigern**.

In den folgenden Abschnitten werden die Berechtigungskategorien erörtert, die Sie im Assistenten Berechtigungseinträge hinzufügen auswählen können.

Vollzugriff

Die Berechtigungen in dieser Kategorie decken alle administrativen Vorgänge für Objekte (und ihre Eigenschaften) der Klassen ab, die Sie im vorigen Schritt des Assistenten Berechtigungseinträge hinzufügen ausgewählt haben.

Wählen Sie **Vollzugriff** aus und klicken Sie auf **Fertig stellen**, um die Berechtigung der neu erstellten Zugriffsvorlage hinzuzufügen.

Objektzugriff

Die Berechtigungen in dieser Kategorie decken alle administrativen Vorgänge für Objekte (jedoch nicht ihre Eigenschaften) der Klassen ab, die Sie im vorigen Schritt des Assistenten Berechtigungseinträge hinzufügen ausgewählt haben.

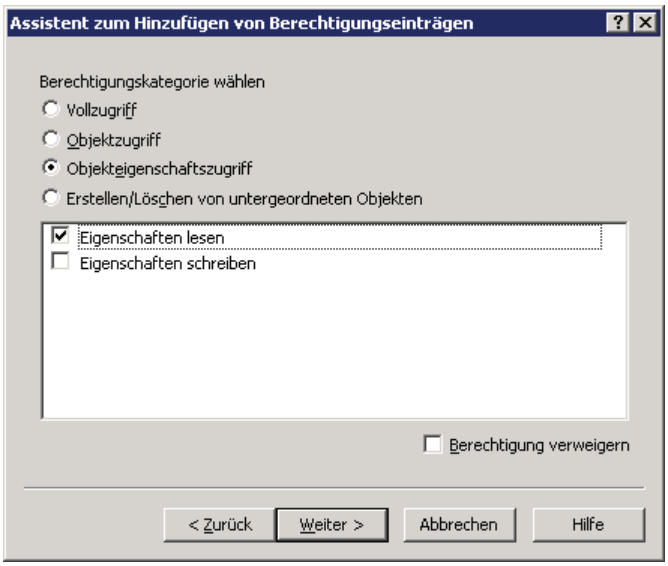
Administrative Vorgänge werden in der Liste ausgewählt, die bei Auswahl von **Objektzugriff** angezeigt wird. Sie wählen die notwendigen Vorgänge aus, indem Sie die entsprechenden Kontrollkästchen aktivieren. Beispielsweise können Sie **Objekt auflisten** auswählen, um das Anzeigen von Objekten bestimmter Typen zuzulassen.

Nachdem Sie die Vorgänge ausgewählt haben, klicken Sie auf **Fertig stellen**, um den Assistent Berechtigungseinträge hinzufügen abzuschließen. Die Berechtigung wird der neu erstellten Zugriffsvorlage hinzugefügt.

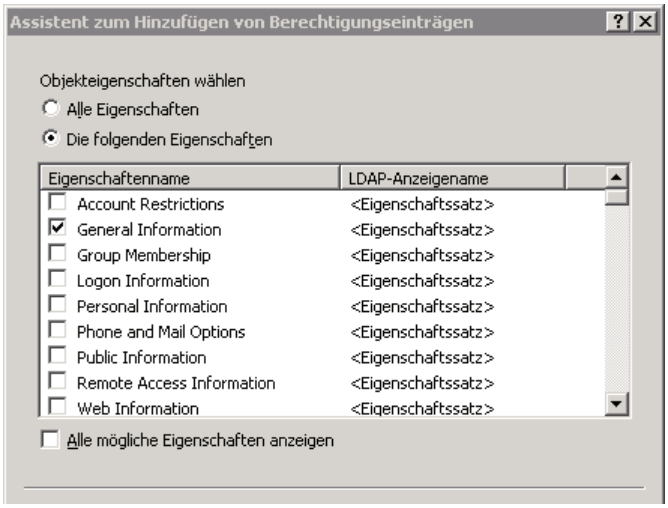
Objekteigenschaftszugriff

Die Berechtigungen in dieser Kategorie decken administrativen Vorgänge für Objekteigenschaften für Objekte der Klassen ab, die Sie im vorigen Schritt des Assistenten Berechtigungseinträge hinzufügen ausgewählt haben.

Wenn Sie **Objekteigenschaftszugriff** auswählen, geben Sie den Zugriff auf Objekteigenschaften an. Sie können **Eigenschaften lesen** und **Eigenschaften schreiben** auswählen, wie in der folgenden Abbildung gezeigt.



Nach dem Klicken auf **Weiter** zeigt der Assistent eine Seite an, auf der Sie die Eigenschaften auswählen können, für die die Berechtigung den Zugriff zulassen (oder verweigern) soll. Die Seite entspricht der folgenden Abbildung:



Auf dieser Seite können Sie eine der folgenden Optionen auswählen:

- **Alle Eigenschaften.** Mit dieser Option steuert die Berechtigung den Zugriff auf alle Eigenschaften.
- **Die folgenden Eigenschaften.** Mit dieser Option steuert die Berechtigung den Zugriff auf die Eigenschaften, die Sie in der Liste auswählen, indem Sie die entsprechenden Kontrollkästchen aktivieren.

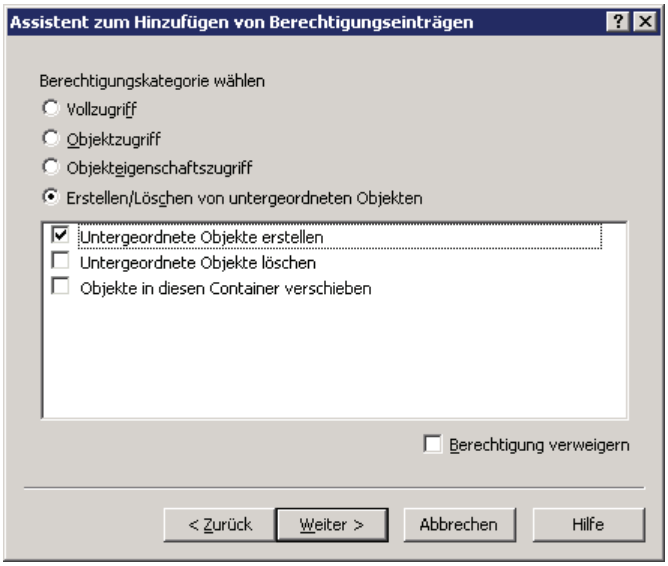
Standardmäßig werden nicht alle Objekteigenschaften in der Liste angezeigt. Um alle Objekteigenschaften anzuzeigen, aktivieren Sie das Kontrollkästchen **Alle mögliche Eigenschaften anzeigen**.

Nachdem Sie die gewünschten Eigenschaften ausgewählt haben, klicken Sie auf **Fertig stellen**, um den Assistent Berechtigungseinträge hinzufügen abzuschließen. Die Berechtigung wird der Zugriffsvorlage hinzugefügt.

Erstellen/Löschen von Berechtigungen für untergeordnete Objekte

Die Berechtigungen in dieser Kategorie decken die Erstellung und Löschung untergeordneter Objekte in Containerobjekten der Klassen ab, die Sie im vorigen Schritt des Assistenten Berechtigungseinträge hinzufügen ausgewählt haben.

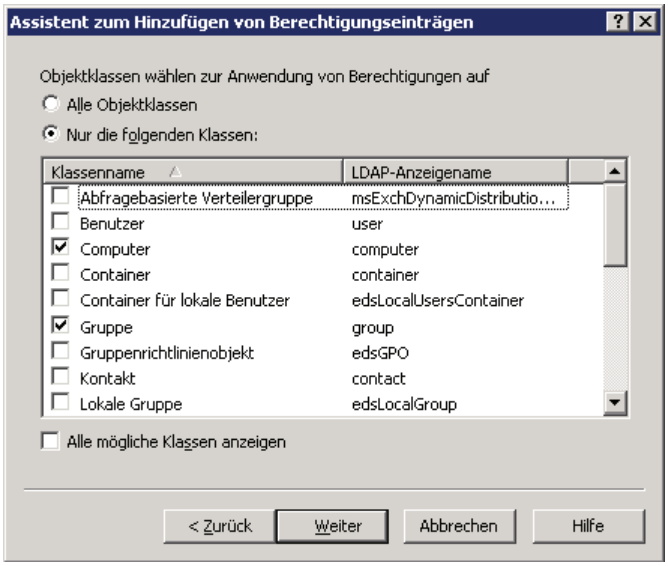
Durch Auswählen von **Erstellen/Löschen von untergeordneten Objekten** geben Sie die Erstellungs-, Lösch- und Verschiebungsvorgänge an, die die Berechtigung zulassen (oder verweigern) soll. Die Liste der Vorgänge wird in der folgenden Abbildung gezeigt.



Sie können folgende Vorgänge wählen:

- **Untergeordnete Objekte erstellen.** Steuert die Erstellung untergeordneter Objekte der Klassen, die Sie im nächsten Schritt auswählen.
- **Untergeordnete Objekte erstellen.** Steuert die Erstellung untergeordneter Objekte der Klassen, die Sie im nächsten Schritt auswählen.
- **Objekte in diesen Container verschieben.** Steuert die Verschiebung von Objekten der Klassen, die Sie im nächsten Schritt auswählen. Für diesen Vorgang wird angenommen, dass Objekte ohne die Berechtigung zum Löschen vorhandener Objekte oder zum Erstellen neuer Objekte von einem Container in einen anderen verschoben werden.

Nach dem Klicken auf **Weiter** zeigt der Assistent die Seite an, auf der Sie die Typen von Objekten auswählen können, für die die Berechtigung die im vorigen Schritt ausgewählten Vorgänge zulassen (oder verweigern) soll. Die Seite entspricht der folgenden Abbildung:



Auf dieser Seite wählen Sie die Typen von Objekten aus, für die Sie mit dieser Berechtigung den Erstellungs-, Lösch- oder Verschiebungsvorgang zulassen (oder verweigern) möchten. Sie können eine der folgenden Optionen auswählen:

- **Alle Objektklassen.** Mit dieser Option steuert die Berechtigung die Vorgänge für Objekte beliebigen Typs.
- **Nur die folgenden Klassen.** Mit dieser Option steuert die Berechtigung die Vorgänge an Objekten des Typs, den Sie in der Liste auswählen, indem Sie die entsprechenden Kontrollkästchen aktivieren.

Standardmäßig werden nicht alle Objektklassen in der Liste angezeigt. Um alle Objektklassen anzuzeigen, aktivieren Sie das Kontrollkästchen **Alle mögliche Klassen anzeigen**.

Nachdem Sie die Objektklassen ausgewählt haben, klicken Sie auf **Fertig** stellen, um den Assistent Berechtigungseinträge hinzufügen abzuschließen. Die Berechtigung wird der Zugriffsvorlage hinzugefügt.

Verfahren zum Erstellen einer Zugriffsvorlage

So erstellen Sie eine Zugriffsvorlage:

1. Machen Sie den Ordner, zu dem Sie die Zugriffsvorlage hinzufügen mochten, in dem Baum der Programmsteuerung unter **Configuration | Access Templates** ausfindig und klicken Sie ihn an.

   *Gehen Sie folgendermaßen vor, um einen neuen Ordner zu erstellen: Klicken Sie mit der rechten Maustaste auf **Access Templates** und wählen Sie dann **New | Access Templates Container**. Auf die gleiche Weise können Sie einen Unterordner in einem Ordner erstellen: Klicken Sie mit der rechten Maustaste auf den Ordner und wählen Sie **New | Access Templates Container** aus.*

2. Klicken Sie mit der rechten Maustaste auf den Ordner und wählen Sie dann **New | Access Template**, um den Assistenten „Neues Objekt - Zugriffsvorlage" zu starten.
3. Gehen Sie auf der ersten Seite des Assistenten wie folgt vor und klicken Sie dann auf **Weiter**:
   a) Geben Sie in das Feld **Name** einen Namen für die Zugriffsvorlage ein.
   b) Geben Sie im Feld **Beschreibung** optionale Informationen über die Zugriffsvorlage ein.
4. Konfigurieren Sie auf der zweiten Seite des Assistenten die Liste der Berechtigungseinträge und klicken Sie dann auf **Weiter**.
   Die Anleitungen bezüglich des Hinzufügens, Änderns oder Löschens von Berechtigungseinträgen sind weiter unten in diesem Thema aufgeführt.
5. Klicken Sie auf **Fertig stellen**, um die Zugriffsvorlage zu erstellen, die die Berechtigungseinträge enthält, die Sie angegeben haben.

Gehen Sie folgendermaßen vor, um einen Berechtigungseintrag zu einer Zugriffsvorlage hinzuzufügen:

1. Klicken Sie auf der Seite, die eine Liste der in der Zugriffsvorlage enthaltenen Berechtigungseinträge anzeigt, auf **Hinzufügen**, um den Assistenten zum Hinzufügen von Berechtigungseinträgen zu starten.
2. Wählen Sie auf der ersten Seite des Assistenten eine der folgenden Optionen aus:
   - **Alle Objektklassen.** Die in diesem Berechtigungseintrag definierten Rechte gelten für Objekte jeglicher Klassen.
   - **Nur die folgenden Klassen.** Die in diesem Berechtigungseintrag definierten Rechte gelten für Objekte bestimmter Klassen. Wählen Sie die Objektklassen aus der Liste aus. Wenn die Liste nicht die gewünschte Objektklasse enthält, wählen Sie **Alle mögliche Klassen anzeigen** aus.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der zweiten Seite des Assistenten eine der folgenden Optionen aus:
   - **Vollzugriff.** Rechte zur Erstellung oder zum Löschen untergeordneter Objekte, zum Lesen und Schreiben von Eigenschaften, zur Untersuchung von untergeordneten Objekten und das Objekt selbst, zum Hinzufügen und Entfernen des Objekts aus dem Verzeichnis und zum Lesen oder Schreiben mit jedem erweiterten Recht. Diese Option verfügt über keine Konfigurationsparameter.
   - **Objektzugriff.** Rechte zur Ausführung von bestimmten, allgemeinen Berechtigungen und erweiterten Rechten für die Objekte. Wählen Sie Berechtigungen und erweiterte Rechte aus der Liste aus, um diese Option wie gewünscht zu konfigurieren.
   - **Objekteigenschaftszugriff.** Rechte zum Lesen oder Schreiben bestimmter Eigenschaften des Objekts. Aktivieren Sie die entsprechenden Kontrollkästchen zur Konfiguration dieser Eigenschaft: **Leseeigenschaften**, **Schreibeigenschaften**. Auf der nächsten Seite des Assistenten können Sie die Eigenschaften auswählen, die durch diesen Berechtigungseintrag kontrolliert werden sollen.
   - **Erstellen/Löschen von untergeordneten Objekten.** Rechte zum Erstellen oder Löschen von untergeordneten Objekten des Objekts. Aktivieren Sie die entsprechenden Kontrollkästchen zur Konfiguration dieser Eigenschaft: **Untergeordnete Objekte erstellen**, **Untergeordnete Objekte löschen**, **Objekte in diesen Container verschieben**. Auf der nächsten Seite des Assistenten können Sie die Klasse oder die Klassen des untergeordneten Objekts auswählen, die durch diesen Berechtigungseintrag kontrolliert werden sollen.
5. Wenn die Zugriffsvorlage die von diesem Berechtigungseintrag definierten Rechte verweigern soll, aktivieren Sie das Kontrollkästchen **Berechtigung verweigern**. Andernfalls muss dieses Kontrollkästchen deaktiviert sein.

6. Führen Sie dann abhängig von der in Schritt 4 ausgewählten und konfigurierten Option eine der folgenden Aktionen aus:
   - **Vollzugriff** oder **Objektzugriff.** Klicken Sie auf **Fertig stellen**, um den Berechtigungseintrag zur Zugriffsvorlage hinzuzufügen.
   - **Objekteigenschaftszugriff** oder **Erstellen/Löschen von untergeordneten Objekten.** Klicken Sie auf **Weiter**, um die Konfiguration der Option fortzusetzen.
7. Setzen Sie auf der dritten Seite des Assistenten die Konfiguration der Option fort, die Sie in Schritt 4 ausgewählt haben, und klicken Sie dann auf **Fertig stellen**, um den Berechtigungseintrag zur Zugriffsvorlage hinzuzufügen:
   - Wenn Sie **Objekteigenschaftszugriff** ausgewählt haben, wählen Sie die Eigenschaften aus, die von diesem Berechtigungseintrag kontrolliert werden sollen. Die beiden folgenden Optionen stehen zur Auswahl: **Alle Eigenschaften** und **Die folgenden Eigenschaften**. Bei Auswahl der zweiten Option müssen Sie Eigenschaften aus der Liste auswählen. Wenn die Liste nicht die gewünschte Eigenschaft enthält, wählen Sie **Alle mögliche Eigenschaften anzeigen** aus.
   - Wenn Sie **Erstellen/Löschen von untergeordneten Objekten** ausgewählt haben, geben Sie die Klasse oder die Klassen des untergeordneten Objekts an, die durch diesen Berechtigungseintrag kontrolliert werden sollen. Die beiden folgenden Optionen stehen zur Auswahl: **Untergeordnete Objekte jeder Klasse** und **Untergeordnete Objekte der folgenden Klassen**. Bei Auswahl der zweiten Option müssen Sie eine oder mehrere Objektklassen aus der Liste auswählen. Wenn die Liste nicht die gewünschte Objektklasse enthält, wählen Sie **Alle mögliche Klassen anzeigen** aus.

Gehen Sie folgendermaßen vor, um einen Berechtigungseintrag in einer Zugriffsvorlage anzuzeigen oder zu ändern:

1. Wählen Sie auf der Seite, die eine Liste der in der Zugriffsvorlage enthaltenen Berechtigungseinträge anzeigt, den Berechtigungseintrag aus, den Sie anzeigen oder ändern möchten, und klicken Sie dann auf **Anzeigen/Bearbeiten**, um das Dialogfeld **Berechtigungseintrag ändern** anzuzeigen.
2. Zeigen Sie die Registerkarte **Übernehmen für** im Dialogfeld **Berechtigungseintrag ändern** an. Auf dieser Registerkarte können Sie dieselben Einstellungen wie auf der ersten Seite des Assistenten zum Hinzufügen von Berechtigungseinträgen anzeigen oder ändern (siehe Schritt 2 im oben beschriebenen Verfahren).
3. Zeigen Sie die Registerkarte **Berechtigungen** im Dialogfeld **Berechtigungseintrag ändern** an. Diese Registerkarte bietet dieselben Optionen wie die zweite Seite des Assistenten zum Hinzufügen von Berechtigungseinträgen (siehe Schritt 4 im oben beschriebenen Verfahren). Die Optionen sind schreibgeschützt; Sie können also die Option nicht ändern, die bei Erstellung des Berechtigungseintrags ausgewählt wurde. Sie können jedoch die Konfiguration der Option verwalten:
   - **Objektzugriff.** Wählen Sie allgemeine Berechtigungen oder erweiterte Rechte aus, die Sie zur Zugriffsvorlage hinzufügen möchten.
   - **Objekteigenschaftszugriff.** Aktivieren oder deaktivieren Sie diese Kontrollkästchen: **Leseeigenschaften**, **Schreibeigenschaften**.
   - **Erstellen/Löschen von untergeordneten Objekten.** Aktivieren oder deaktivieren Sie diese Kontrollkästchen: **Untergeordnete Objekte erstellen**, **Untergeordnete Objekte löschen**, **Objekte in diesen Container verschieben**.
4. Wenn die Zugriffsvorlage die von diesem Berechtigungseintrag definierten Rechte verweigern soll, aktivieren Sie das Kontrollkästchen **Berechtigung verweigern** auf der Registerkarte **Berechtigungen**. Andernfalls muss dieses Kontrollkästchen deaktiviert sein.
5. Wenn **Objekteigenschaftszugriff** auf der Registerkarte **Berechtigungen** aktiviert ist, verwenden Sie die Registerkarte **Objekteigenschaften** im Dialogfeld **Berechtigungseintrag ändern**, um die Einstellungen anzuzeigen oder zu ändern, die festlegen, welche Eigenschaften durch diesen Berechtigungseintrag kontrolliert werden (siehe Schritt 7 im oben beschriebenen Verfahren).

6. Wenn **Erstellung/Löschen von untergeordneten Objekte** auf der Registerkarte **Berechtigungen** ausgewählt ist, verwenden Sie die Registerkarte **Objektklassen** im Dialogfeld **Berechtigungseintrag ändern**, um die Einstellungen anzuzeigen oder zu ändern, die festlegen, welche untergeordnete Objektklassen durch diesen Berechtigungseintrag kontrolliert werden.

Gehen Sie folgendermaßen vor, um einen Berechtigungseintrag aus einer Zugriffsvorlage zu löschen:

1. Wählen Sie auf der Seite, die eine Liste der in der Zugriffsvorlage enthaltenen Berechtigungseinträge anzeigt, den Berechtigungseintrag aus, den Sie löschen möchten, und klicken Sie dann auf **Entfernen**.
2. Klicken Sie auf **Ja**, um den Löschvorgang zu bestätigen.

Anwenden von Zugriffsvorlagen

Quest One ActiveRoles ermöglicht die Anwendung der Zugriffsvorlagen auf alle Objekt Verwaltungsansichten (verwaltete Einheiten), Verzeichnisordner (Container) oder einzelne (Blatt-) Objekte.

Beim Anwenden einer Zugriffsvorlage auf ein Objekt wählen Sie einen Trustee (Benutzer oder Gruppe) aus und weisen dem Trustee für dieses Objekt Berechtigungen zu. Folglich erhält der Trustee Zugriff auf das Objekt gemäß den in der Zugriffsvorlage definierten Berechtigungen.

So kann beispielsweise zwei Assistenten eines Verzeichnisadministrators ein Vollzugriff auf verschiedene Domänen gewährt werden. Dem Help Desk kann eine Administratorfunktion zum Zurücksetzen von Kennwörtern zugewiesen werden.

Wenn Sie Zugriffsvorlagen auf einen Ordner anwenden, können Sie die Berechtigungseinstellungen so konfigurieren, dass sie von dem Ordner an seine untergeordneten Objekte weiter unten in der Verzeichnisstruktur weitergegeben werden.

Zum Anwenden einer Zugriffsvorlage müssen Sie den Assistenten zum Delegieren der Kontrolle starten und abschließen.

Sie können den Assistenten zum Delegieren der Kontrolle von jeder der nachfolgend aufgeführten Positionen starten:

- **Zugriffsvorlage.** Klicken Sie mit der rechten Maustaste auf die Zugriffsvorlage, klicken Sie dann auf **Verknüpfungen** und anschließend auf die Schaltfläche **Hinzufügen**. Zugriffsvorlagen befinden sich im Container **Configuration/Access Templates**.

  Wenn der Assistent auf diese Weise gestartet wird, können Sie Verzeichnisobjekte auswählen, in denen die Zugriffsvorlage und die Trustees für diese Objekte angewendet werden sollen.

- **Sicherbares Objekt.** Abhängig davon, ob das Objekt ein Container- oder ein Blattobjekt ist, führen Sie eine der folgenden Aktionen aus:

  - Wenn es sich um einen Container oder eine verwaltete Einheit handelt, klicken Sie mit der rechten Maustaste darauf, klicken Sie auf **Kontrolle delegieren** und klicken Sie dann auf die Schaltfläche **Hinzufügen**.
  - Wenn es sich um ein Blattobjekt handelt, zeigen Sie das Dialogfeld **Eigenschaften** an, wechseln Sie zur Registerkarte **Verwaltung**, klicken Sie auf die Schaltfläche **Sicherheit** und dann auf die Schaltfläche **Hinzufügen**.

  Wenn der Assistent auf diese Weise gestartet wird, können Sie Trustees für das Objekt sowie Zugriffsvorlagen auswählen, in denen die Rechte der Trustees für das Objekt definiert werden sollen.

- **Sicherheitsprinzipal (Trustee).** Klicken Sie mit der rechten Maustaste auf die Gruppe oder den Benutzer, die bzw. den Sie als Trustee auswählen möchten, klicken Sie auf **Delegierte Rechte** und klicken Sie dann auf die Schaltfläche „Hinzufügen".

  Wenn der Assistent auf diese Weise gestartet wird, können Sie Objekte auswählen, für die Sie den Trustee und die Zugriffsvorlagen auswählen möchten, in denen die Rechte der Trustees für diese Objekte definiert werden sollen.

Sie können den Assistenten Delegation der Kontrolle auch vom erweiterten Bereich „Details" aus starten (stellen Sie sicher, dass **Erweiterte Detailansicht** im Menü **Ansicht** aktiviert ist):

- Wählen Sie eine Zugriffsvorlage aus, klicken Sie mit der rechten Maustaste in einen leeren Bereich auf der Registerkarte **Verknüpfungen** und klicken Sie dann auf **Hinzufügen**.

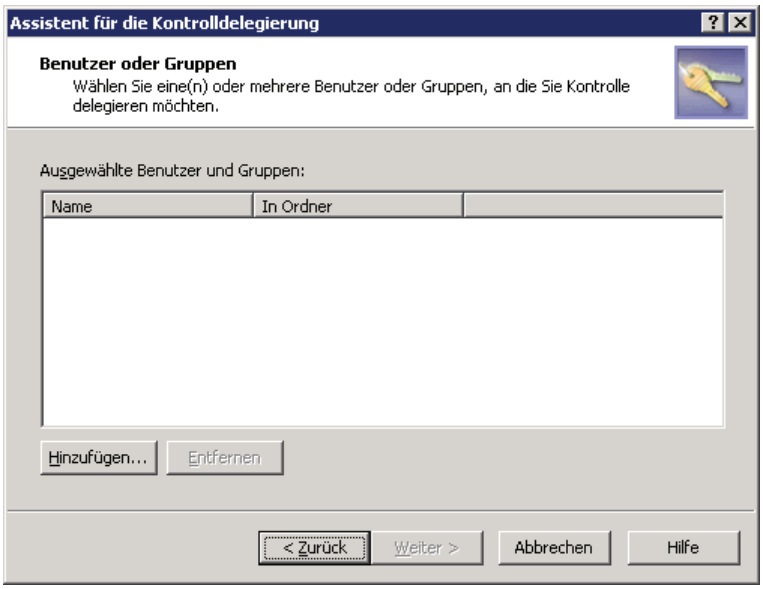
  Wenn der Assistent auf diese Weise gestartet wird, können Sie Verzeichnisobjekte auswählen, in denen die Zugriffsvorlage und die Trustees für diese Objekte angewendet werden sollen.

- Wahlen Sie ein Verzeichnisobjekt (zu sicherndes Objekt) aus, klicken Sie mit der rechten Maustaste in einen leeren Bereich auf der Registerkarte **ActiveRoles-Sicherheit** und dann mit links auf **Hinzufügen**.

  Wenn der Assistent auf diese Weise gestartet wird, können Sie Trustees für das Objekt sowie Zugriffsvorlagen auswählen, in denen die Rechte der Trustees für das Objekt definiert werden sollen.

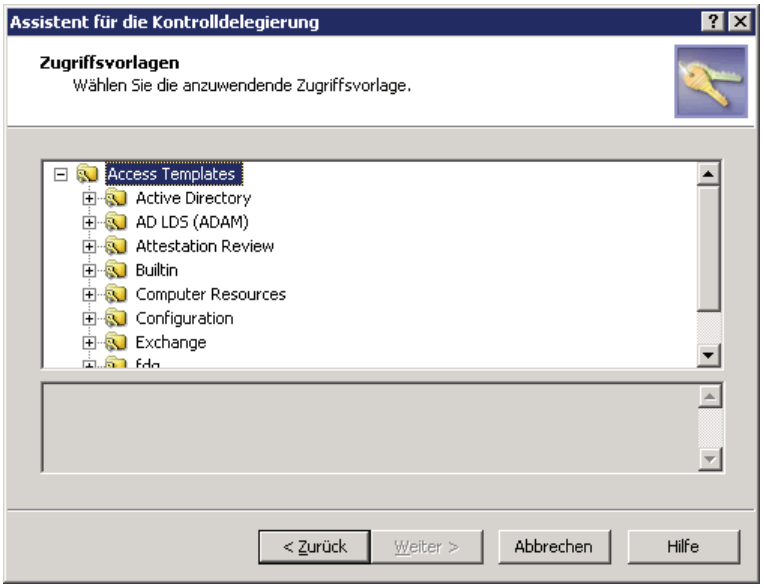
Der Rest dieses Abschnitts enthält Anweisungen zum Abschließen des Assistenten Delegation der Kontrolle. Dabei wird angenommen, dass Sie den Assistenten von dem Objekt aus starten, für das Sie die Kontrolle delegieren möchten (von einem sicherbaren Objekt). Anweisungen bezüglich der Fertigstellung des Assistenten in den anderen Fällen finden Sie unter Verfahren zum Anwenden einer Zugriffsvorlage weiter unten in diesem Kapitel.

Wenn Sie den „Assistent für die Kontrolldelegierung" ausgehend von einem sicherbaren Objekt starten, wird durch Anklicken von **Weiter** auf der Seite **Willkommen** die Seite **Benutzer oder Gruppen** angezeigt, die in der folgenden Abbildung dargestellt ist.



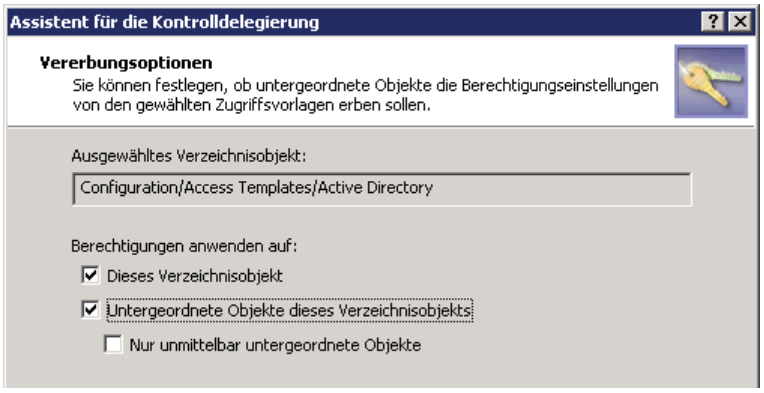
Klicken Sie auf der Seite **Benutzer oder Gruppen** auf **Hinzufügen**, um das Dialogfeld **Objekte auswählen** anzuzeigen, in dem Sie Gruppen oder Benutzer auswählen können, die zu Trustees ernannt werden sollen. Geben Sie die Namen der Benutzer oder Gruppen, die Sie zur Liste hinzufügen möchten, ein oder wählen Sie diese aus und klicken Sie dann auf **OK**.

Klicken Sie nach dem Abschließen der Liste auf der Seite **Benutzer oder Gruppen** auf **Weiter**. Nun wird die Seite **Zugriffsvorlagen** angezeigt, die in der folgenden Abbildung gezeigt wird.



Erweitern Sie auf der Seite **Zugriffsvorlagen** Container, die Zugriffsvorlagen enthalten, und aktivieren Sie Kontrollkästchen neben den Namen der Zugriffsvorlagen, die Sie anwenden möchten.

Klicken Sie nach dem Auswählen aller gewünschten Zugriffsvorlagen auf **Weiter**. Nun wird die Seite **Vererbungsoptionen** angezeigt, die in der folgenden Abbildung gezeigt wird.


Assistent für die Kontrolldelegierung
Vererbungsoptionen
Sie können festlegen, ob untergeordnete Objekte die Berechtigungseinstellungen von den gewählten Zugriffsvorlagen erben sollen.
Ausgewähltes Verzeichnisobjekt:
Configuration/Access Templates/Active Directory
Berechtigungen anwenden auf:
Dieses Verzeichnisobjekt
Untergeordnete Objekte dieses Verzeichnisobjekts
Nur unmittelbar untergeordnete Objekte

Auf der Seite **Vererbungsoptionen** können Sie die folgenden Optionen auswählen, um die Vererbung von Berechtigungen zu kontrollieren:

- **Dieses Verzeichnisobjekt.** Stellt sicher, dass die Trustees über Administratorrechte für das sicherbare Objekt selbst verfügen.

- **Untergeordnete Objekte dieses Verzeichnisobjekts.** Stellt sicher, dass die Trustees über Administratorrechte für die untergeordneten Objekte des sicherbaren Objekts verfügen, die in der Verzeichnisstruktur unter ihm liegen.
- **Nur unmittelbar untergeordnete Objekte.** Beschränkt die Rechte der Trustees auf die unmittelbar untergeordneten Objekte des sicherbaren Objekts.

Standardmäßig sind die ersten beiden Optionen ausgewählt.

Klicken Sie auf **Weiter**. Daraufhin erscheint die Seite zur **Weitergabe der Berechtigungen**, auf dieser kann ein Haken in das Kästchen **Berechtigungen an Active Directory weitergeben** gesetzt werden. Wenn Sie es aktivieren, werden die Berechtigungseinstellungen, die Sie konfigurieren, nach Active Directory synchronisiert. Infolgedessen dürfen die Bevollmächtigten ihre Rechte auch außerhalb der Quest One ActiveRoles-Umgebung ausüben, woraus die Gefahr einer möglichen Umgehung der für Quest One ActiveRoles aufgestellten und durchgesetzten Richtlinien erwachst. Daher sollten Sie diese Option wohl überlegt verwenden.

Standardmäßig ist das Kontrollkästchen **Berechtigungen an Active Directory weitergeben** deaktiviert. Wenn Sie sich für diese Möglichkeit entscheiden, können Sie diese Einstellung jederzeit mithilfe der Schaltflache **Mit AD synchronisieren** im **Quest One ActiveRoles Sicherheit**sfenster oder durch den Befehl **Mit AD synchronisieren** im Fenster der erweiterten Angaben ändern (siehe Synchronisieren von Berechtigungen mit Active Directory weiter hinten in diesem Kapitel).

Klicken Sie auf **Weiter** und klicken Sie dann auf **Fertig stellen**, um den Assistenten abzuschließen.

Verfahren zum Anwenden einer Zugriffsvorlage

So wenden Sie eine Zugriffsvorlage an:

1. Machen Sie den Ordner, der die Zugriffsvorlage, die Sie anwenden mochten, enthalt, in dem Baum der Programmsteuerung unter **Einrichtungseinstellungen | Zugriffsvorlagen** ausfindig und klicken Sie ihn an.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf die Zugriffsvorlage und klicken Sie dann auf **Verknüpfungen**.
3. Klicken Sie im Dialogfeld **Verknüpfungen** auf **Hinzufügen**, um den Assistenten zum Delegieren der Kontrolle zu starten.
4. Klicken Sie auf der Seite Willkommen des Assistenten auf **Weiter**.
5. Fügen Sie auf der Seite **Objekte** die Objekte hinzu, für die Sie Berechtigungseinstellungen mit Hilfe der Zugriffsvorlage festlegen möchten, oder entfernen Sie sie aus der Seite:
   - Um Objekte hinzuzufügen, klicken Sie auf **Hinzufügen** und verwenden Sie dann das Dialogfeld **Objekte auswählen**, um die Objekte auszuwählen.
   - Um Objekte zu entfernen, wählen Sie diese in der Liste auf der Seite **Objekte** aus und klicken Sie dann auf **Entfernen**.
6. Klicken Sie auf **Weiter**.
7. Fügen Sie auf der Seite **Benutzer oder Gruppen** die Benutzer oder Gruppen (Trustee) hinzu bzw. entfernen Sie sie, denen Sie die Berechtigungen zuordnen möchten, die von der Zugriffsvorlage für die Objekte, die Sie auf der Seite **Objekte** aufgenommen haben, definiert sind:
   - Um Benutzer oder Gruppen hinzuzufügen, klicken Sie auf **Hinzufügen** und verwenden Sie dann das Dialogfeld **Objekte auswählen**, um die Benutzer oder Gruppen auszuwählen.
   - Um Benutzer oder Gruppen zu entfernen, wählen Sie diese in der Liste auf der Seite **Benutzer oder Gruppen** aus und klicken Sie dann auf **Entfernen**.

8. Klicken Sie auf **Weiter**.
9. Aktivieren bzw. deaktivieren Sie auf der Seite **Vererbungsoptionen** die entsprechenden Kontrollkästchen:
   - **Dieses Verzeichnisobjekt.** Geben Sie Berechtigungseinstellungen für die Objekte an, die Sie auf der Seite **Objekte** aufgenommen haben.
   - **Untergeordnete Objekte dieses Verzeichnisobjekts.** Geben Sie Berechtigungseinstellungen für alle untergeordneten Objekte (oder Mitglieder bei einer verwalteten Einheit) in der gesamten Hierarchie unter jedem der Objekte an, die Sie auf der Seite **Objekte** aufgenommen haben.
   - **Nur unmittelbar untergeordnete Objekte.** Geben Sie Berechtigungseinstellungen nur für die untergeordneten Objekte (oder Mitglieder bei einer verwalteten Einheit) an, von denen die Objekte, die Sie auf der Seite **Objekte** aufgenommen haben, direkt übergeordnete Objekte sind.
10. Klicken Sie auf **Weiter**.
11. Wählen Sie auf der Seite **Berechtigungsverbreitung** die Option **Berechtigungen an Active Directory verbreiten** aus, wenn die auf Zugriffsvorlagen basierenden Berechtigungseinstellungen mit den nativen Active Directory-Zugriffskontrollen synchronisiert werden sollen. Das fuhrt zu der Änderung der Berechtigungsangaben bezüglich der Objekte in Active Directory auf der Grundlage der in Quest One ActiveRoles festgelegten Berechtigungseinstellungen.
12. Klicken Sie auf **Weiter**.
13. Klicken Sie auf **Fertig stellen**.

Gehen Sie folgendermaßen vor, um die Berechtigungseinstellungen für ein Objekt mit Hilfe einer Zugriffsvorlage anzugeben:

1. Anzeigen des Dialogfeldes **Quest One ActiveRoles-Sicherheit** für das Objekt:
   - Klicken Sie mit der rechten Maustaste auf das Objekt und klicken Sie dann auf **Kontrolle delegieren**.

   – ODER –

   - Klicken Sie mit der rechten Maustaste auf das Objekt und klicken Sie dann auf **Eigenschaften**. Klicken Sie dann auf der Registerkarte **Verwaltung** im Dialogfeld **Eigenschaften** auf **Sicherheit**.
2. Zum Aufrufen des Assistenten zur Delegierung der Überwachung klicken Sie in dem Dialogfeld **Quest One ActiveRoles-Sicherheit** auf **Hinzufügen**.
3. Klicken Sie auf der Seite Willkommen des Assistenten auf **Weiter**.
4. Fügen Sie auf der Seite **Benutzer oder Gruppen** die Benutzer oder Gruppen (Trustee), denen Sie die Berechtigungen für das Objekt zuordnen möchten, hinzu bzw. entfernen Sie sie:
   - Um Benutzer oder Gruppen hinzuzufügen, klicken Sie auf **Hinzufügen** und verwenden Sie dann das Dialogfeld **Objekte auswählen**, um die Benutzer oder Gruppen auszuwählen.
   - Um Benutzer oder Gruppen zu entfernen, wählen Sie diese in der Liste auf der Seite **Benutzer oder Gruppen** aus und klicken Sie dann auf **Entfernen**.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Zugriffsvorlagen** die anzuwendende Zugriffsvorlage aus.
   Sie können mehrere anzuwendende Zugriffsvorlagen auswählen.
7. Klicken Sie auf **Weiter**.

8. Aktivieren bzw. deaktivieren Sie auf der Seite **Vererbungsoptionen** die entsprechenden Kontrollkästchen:
   - **Dieses Verzeichnisobjekt.** Geben Sie Berechtigungseinstellungen für das Objekt selbst an.
   - **Untergeordnete Objekte dieses Verzeichnisobjekts.** Geben Sie Berechtigungseinstellungen für alle untergeordneten Objekte (oder Mitglieder bei einer verwalteten Einheit) in der gesamten Hierarchie unter dem Objekt an.
   - **Nur unmittelbar untergeordnete Objekte.** Geben Sie Berechtigungseinstellungen nur für die untergeordneten Objekte (oder Mitglieder bei einer verwalteten Einheit) an, denen das Objekt direkt übergeordnet ist.
9. Klicken Sie auf **Weiter**.
10. Wählen Sie auf der Seite **Berechtigungsverbreitung** die Option **Berechtigungen an Active Directory verbreiten** aus, wenn die auf Zugriffsvorlagen basierenden Berechtigungseinstellungen mit den nativen Active Directory-Zugriffskontrollen synchronisiert werden sollen. Das fuhrt zu der Änderung der Berechtigungsangaben bezüglich des Objekts in Active Directory auf der Grundlage der in Quest One ActiveRoles festgelegten Berechtigungseinstellungen.
11. Klicken Sie auf **Weiter**.
12. Klicken Sie auf **Fertig stellen**.

Gehen Sie folgendermaßen vor, um Berechtigungen für einen Benutzer oder eine Gruppe mit Hilfe der Zugriffsvorlage anzugeben:

1. Klicken Sie mit der rechten Maustaste auf den Benutzer oder die Gruppe und klicken Sie dann auf **Delegierte Rechte**.
2. Klicken Sie im Dialogfeld **Delegierte Rechte** auf **Hinzufügen**, um den Assistenten zum Delegieren der Kontrolle zu starten.
3. Klicken Sie auf der Seite Willkommen des Assistenten auf **Weiter**.
4. Fügen Sie auf der Seite **Objekte** die Objekte hinzu, für die Sie Berechtigungen für den Benutzer oder die Gruppe festlegen möchten:
   - Um Objekte hinzuzufügen, klicken Sie auf **Hinzufügen** und verwenden Sie dann das Dialogfeld **Objekte auswählen**, um die Objekte auszuwählen.
   - Um Objekte zu entfernen, wählen Sie diese in der Liste auf der Seite **Objekte** aus und klicken Sie dann auf **Entfernen**.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Zugriffsvorlagen** die anzuwendende Zugriffsvorlage aus.

   Sie können mehrere anzuwendende Zugriffsvorlagen auswählen.
7. Klicken Sie auf **Weiter**.
8. Aktivieren bzw. deaktivieren Sie auf der Seite **Vererbungsoptionen** die entsprechenden Kontrollkästchen:
   - **Dieses Verzeichnisobjekt.** Geben Sie Berechtigungen für die Objekte an, die Sie auf der Seite **Objekte** aufgenommen haben.
   - **Untergeordnete Objekte.** Dieses Verzeichnisobjekts. Geben Sie Berechtigungen für alle untergeordneten Objekte (oder Mitglieder bei einer verwalteten Einheit) in der gesamten Hierarchie unter jedem der Objekte an, die Sie auf der Seite **Objekte** aufgenommen haben.
   - **Nur unmittelbar untergeordnete Objekte.** Geben Sie Berechtigungen nur für die untergeordneten Objekte (oder Mitglieder bei einer verwalteten Einheit) an, von denen die Objekte, die Sie auf der Seite **Objekte** aufgenommen haben, direkt übergeordnete Objekte sind.
9. Klicken Sie auf **Weiter**.

10. Wählen Sie auf der Seite **Berechtigungsverbreitung** die Option **Berechtigungen an Active Directory verbreiten** aus, wenn die auf Zugriffsvorlagen basierenden Berechtigungseinstellungen mit den nativen Active Directory-Zugriffskontrollen synchronisiert werden sollen. Das fuhrt zu der Änderung der Berechtigungsangaben bezüglich der Objekte in Active Directory auf der Grundlage der in Quest One ActiveRoles festgelegten Berechtigungseinstellungen.
11. Klicken Sie auf **Weiter**.
12. Klicken Sie auf **Fertig stellen**.

- Quest One ActiveRoles ermöglicht die Anwendung von Zugriffsvorlagen auf alle Objekte einschließlich verwaltete Einheiten, Verzeichnisordner (Container) und einzelne (Blatt-) Objekte.
- Beim Anwenden einer Zugriffsvorlage auf ein Objekt wählen Sie einen Trustee (Benutzer oder Gruppe) aus und weisen dem Trustee für dieses Objekt Berechtigungen zu. Der Trustee erhält dadurch Zugriff auf das Objekt entsprechend den Berechtigungen, die durch die Zugriffsvorlage definiert wurden.
- Um eine Zugriffsvorlage anzuwenden, nutzen Sie den Assistenten zum Delegieren der Kontrolle. Sie können den Assistenten wie in diesem Thema beschrieben starten. Der Assistent kann auch über die Registerkarten **Verknüpfungen (Links)** oder **ActiveRoles-Sicherheit** im Fenster der erweiterten Angaben aufgerufen werden: Klicken Sie mit der rechten Maustaste auf einen freien Bereich auf der Registerkarte und klicken Sie dann auf **Hinzufügen**. Um die erweiterte Detailanzeige anzuzeigen, aktivieren Sie **Erweiterte Detailansicht** im Menü **Ansicht** (siehe Erweiterter Bereich weiter oben in diesem Dokument).

Verwalten von Zugriffsvorlagenverknüpfungen

Wenn eine Zugriffsvorlage angewendet wird, legt Quest One ActiveRoles eine Verknüpfung für diese Zugriffsvorlage an. Administratorrechte werden also durch Verknüpfen von Zugriffsvorlagen mit sicherbaren Objekten angegeben, d.h. mit verwalteten Einheiten, Verzeichnisordnern (Containern) oder einzelnen Objekten (Blattobjekten).

Jede Zugriffsvorlagenverknüpfung umfasst den Bezeichner (Security ID, SID) des Sicherheitsprinzipals (des Benutzers oder der Gruppe), dem die angegebenen Administratorrechte zugewiesen sind. Bei der Erstellung einer Zugriffsvorlagenverknüpfung wird der Benutzer oder die Gruppe zum Trustee für die Objektauflistung oder den Ordner, mit dem die Zugriffsvorlage verknüpft ist. Die Berechtigungen werden dabei durch diese Zugriffsvorlage angegeben.

Wenn eine Zugriffsvorlage geändert oder nicht mehr angewendet wird, werden die Berechtigungsinformationen für Objekte, auf die sich die Zugriffsvorlage auswirkt, entsprechend geändert.

Sie können über eine der folgenden Möglichkeiten eine Liste von Zugriffsvorlagenverknüpfungen anzeigen:

- **Zugriffsvorlage.** Klicken Sie mit der rechten Maustaste auf eine Zugriffsvorlage und klicken Sie dann auf **Verknüpfungen**.

  Dies zeigt die Verknüpfungen an, in denen die Zugriffsvorlage auftritt.

- **Sicherheitsprinzipal (Trustee).** Klicken Sie mit der rechten Maustaste auf eine Gruppe oder einen Benutzer und klicken Sie dann auf **Delegierte Rechte**.

  Dann werden die Verknüpfungen angezeigt, in denen die Gruppe oder der Benutzer direkt oder aufgrund von Gruppenmitgliedschaften als Trustee auftritt.

- **Sicherbares Objekt.** Klicken Sie mit der rechten Maustaste auf ein Containerobjekt oder eine verwaltete Einheit und klicken Sie dann auf **Kontrolle delegieren**. Für ein Blattobjekt öffnen Sie das Dialogfeld **Eigenschaften**, öffnen die Registerkarte **Verwaltung** und klicken auf **Sicherheit**.

  Dann werden die Verknüpfungen angezeigt, in denen das ausgewählte Objekt als sicherbares Objekt (bezeichnet als *Verzeichnisobjekt*) auftritt.

Sie können eine Liste von Zugriffsvorlagenverknüpfungen auch im erweiterten Bereich „Details" anzeigen. Stellen Sie sicher, dass im Menü **Ansicht** die Option **Erweiterte Detailansicht** aktiviert ist, und wählen Sie dann eine der folgenden Möglichkeiten aus:

- Zugriffsvorlage

  Auf der Registerkarte **Verknüpfungen** werden die Verknüpfungen aufgelistet, in denen die ausgewählte Zugriffsvorlage auftritt.

- Anderes Objekt (verwaltete Einheit, Container oder Blattobjekt)

  Auf der Registerkarte **ActiveRoles-Sicherheit** werden die Verknüpfungen aufgeführt, in denen das ausgewählte Objekt als zu sicherndes Objekt erscheint (und als Verzeichnisobjekt bezeichnet wird).

In der Programmsteuerung von Quest One ActiveRoles wird eine Aufstellung der Zugriffsvorlagenverknupfungen in einem gesonderten Fenster angezeigt. Aus diesem Grund wird das **Quest One ActiveRoles-Sicherheit**sfenster angezeigt, wenn das Programm von einem zu sichernden Objekt aus aufgerufen wird (wenn Sie zum Beispiel eine verwaltete oder eine Organisationseinheit anklicken und anschließend **Überwachung delegieren**).

Jeder Eintrag in der Aufstellung der Zugriffsvorlagenverknupfungen beinhaltet folgende Angaben:

- **Vertrauensnehmer.** Die Verknüpfung definiert Administratorrechte dieses Sicherheitsprinzipals (Gruppe oder Benutzer).
- **Zugriffsvorlage.** Die Zugriffsvorlage, die die Rechte des Trustees bestimmt.
- **Verzeichnisobjekt.** Die Verknüpfung definiert die Rechte des Trustees für dieses sicherbare Objekt.
- **Mit interner Sicherheit synchronisieren.** Hier wird angezeigt, ob Quest One ActiveRoles die Berechtigungen mit Active Directory synchronisiert oder nicht.
- **Deaktiviert.** Gibt an, ob die Berechtigungen tatsächlich angewendet werden. Wenn eine Verknüpfung deaktiviert ist, kann der Trustee die Administratorrechte nicht ausüben, die durch sie definiert werden.

Im **Quest One ActiveRoles-Sicherheit**sfenster (sowie in der Registerkarte **ActiveRoles-Sicherheit** im Fenster der erweiterten Angaben) werden die Verknüpfungen folgender Kategorien aufgeführt:

- **Direkte Verknüpfungen.** Die Zugriffsvorlage wird direkt auf das ausgewählte sicherbare Objekt angewendet (mit ihm verknüpft).
- **Geerbte Verknüpfungen.** Die Zugriffsvorlage wird auf einen Container in der Containerhierarchie über dem ausgewählten sicherbaren Objekt oder auf eine verwaltete Einheit, zu der das sicherbare Objekt gehört, angewendet (mit ihm/ihr verknüpft).

Die von übergeordneten Objekte geerbten Verknüpfungen können aus der Liste herausgefiltert werden:

- Entfernen Sie bei der Verwendung des Fensters **Quest One ActiveRoles-Sicherheit** den Haken in dem Kästchen **Übernommene anzeigen**.
- Klicken Sie, wenn Sie die Registerkarte **ActiveRoles-Sicherheit** verwenden, mit der rechten Maustaste auf die Aufstellung und dann mit links auf **Übernommene anzeigen**, um den Haken bei diesem Menüpunkt zu entfernen.

In einem Fenster oder auf einer Registerkarte, wo Zugriffsvorlagenverknüpfungen angezeigt werden, können Sie Verknüpfungen verwalten. In einem Fenster können Sie die Schaltflächen unter der Liste verwenden. Auf einer Registerkarte können Sie mit der rechten Maustaste auf einen Listeneintrag oder in einen leeren Bereich klicken und dann Befehle im Kontextmenü verwenden. In dem **Quest One ActiveRoles-Sicherheit**sfenster werden zum Beispiel folgende Schaltflachen angezeigt:

- **Hinzufügen.** Startet den Assistenten Delegation der Kontrolle für die Erstellung/Anwendung von Zugriffsvorlagen.
- **Entfernen.** Löscht die ausgewählten Einträge aus der Verknüpfungsliste. Nur für direkte Verknüpfungen verfügbar.
- **Anzeigen/Bearbeiten.** Zeigt das Dialogfeld an, in dem Verknüpfungseigenschaften angezeigt oder geändert werden können, z.B. Optionen für die Vererbung und die Weitergabe von Berechtigungen.
- **Mit AD synchronisieren.** Schaltet die Option für die Berechtigungsweitergabe für die in der Liste ausgewählten Verknüpfungen um.
- **Deaktivieren.** Deaktiviert oder aktiviert die Verknüpfung. Wenn eine Verknüpfung deaktiviert ist, haben die von ihr angegebenen Berechtigungen keine Auswirkungen.

Im Fenster der **Quest One ActiveRoles-Sicherheit** ist die Schaltflache **Entfernen** ausschließlich bei unmittelbaren Verknüpfungen verfügbar. Wenn Sie Verknüpfungen löschen möchten, sollten Sie sie mit dem Befehl **Verknüpfungen** für die Zugriffsvorlage verwalten.

Verfahren zum Verwalten von Zugriffsvorlagenverknüpfungen

Wenn eine Zugriffsvorlage angewendet wird (siehe Anwenden von Zugriffsvorlagen weiter vorne in diesem Dokument), legt Quest One ActiveRoles ein als *Zugriffsvorlagenverknüpfung*, bezeichnetes Objekt an, in dem die Angaben zu der Zugriffsvorlage sowie zu dem Verzeichnisobjekt, auf das sie angewendet wird, und zu dem Benutzer oder der Gruppe (verallgemeinert: der Bevollmächtigte), denen die Berechtigungen zugewiesen wurden, gespeichert werden. Im Grunde lauft die Verwaltung der Berechtigungseinstellungen in Quest One ActiveRoles auf die Verwaltung von Zugriffsvorlagen und deren Verknüpfungen hinaus. In diesem Thema sind einige Anleitungen aufgeführt, die Sie zum Anzeigen und Ändern von Zugriffsvorlagenverknüpfungen verwenden können.

Gehen Sie folgendermaßen vor, um Zugriffsvorlagenverknüpfungen anzuzeigen oder zu ändern, in denen eine bestimmte Zugriffsvorlage vorkommt:

1. Klicken Sie mit der rechten Maustaste auf Zugriffsvorlage und klicken Sie dann auf **Verknüpfungen**.
2. Nehmen Sie im Dialogfeld **Verknüpfungen** Folgendes vor:
   - Um eine neue Verknüpfung zu erstellen, klicken Sie auf **Hinzufügen** und folgen Sie den Anweisungen im Assistenten zum Delegieren der Kontrolle, um eine Zugriffsvorlage anzuwenden (Anweisungen finden Sie unter Verfahren zum Anwenden einer Zugriffsvorlage weiter oben in diesem Dokument).
   - Um eine Verknüpfung zu löschen, wählen Sie sie aus der Liste aus und klicken Sie dann auf **Entfernen**.

- Um die Vererbungs- und Synchronisationseinstellungen für eine Verknüpfung anzuzeigen oder zu ändern, wählen Sie die Verknüpfung aus und klicken Sie dann auf **Anzeigen/ Bearbeiten**.
- Um die Synchronisationseinstellung für eine Verknüpfung zu ändern, wählen Sie die Verknüpfung aus und klicken Sie dann auf **Mit AD synchronisieren** oder **Desynchronisieren mit AD**.
- Um die Auswirkungen einer Verknüpfung zu entfernen oder wiederherzustellen, wählen Sie die Verknüpfung aus und klicken Sie dann auf **Deaktivieren** bzw. **Aktivieren**.

Gehen Sie folgendermaßen vor, um Zugriffsvorlagenverknüpfungen anzuzeigen oder zu ändern, die die Berechtigungseinstellungen für ein bestimmtes Objekt bestimmen:

1. Anzeigen des Dialogfeldes **Quest One ActiveRoles-Sicherheit** für das Objekt:
   - Klicken Sie mit der rechten Maustaste auf das Objekt und klicken Sie dann auf **Kontrolle delegieren**.

   – ODER –

   - Klicken Sie mit der rechten Maustaste auf das Objekt und klicken Sie dann auf **Eigenschaften**. Klicken Sie dann auf der Registerkarte **Verwaltung** im Dialogfeld **Eigenschaften** auf **Sicherheit**.
2. Tun Sie im Dialogfeld **Quest One ActiveRoles-Sicherheit** Folgendes:
   - Um eine neue Verknüpfung zu erstellen, klicken Sie auf **Hinzufügen** und befolgen dann die Anweisungen im Assistenten zum Delegieren der Kontrolle, um Berechtigungseinstellungen für das Objekt mit Hilfe einer Zugriffsvorlage festzulegen (Anweisungen finden Sie im Abschnitt Verfahren zum Anwenden einer Zugriffsvorlage weiter oben in diesem Dokument).
   - Um eine Verknüpfung zu löschen, wählen Sie sie aus der Liste aus und klicken Sie dann auf **Entfernen**.
   - Um die Vererbungs- und Synchronisationseinstellungen für eine Verknüpfung anzuzeigen oder zu ändern, wählen Sie die Verknüpfung aus und klicken Sie dann auf **Anzeigen/ Bearbeiten**.
   - Um die Synchronisationseinstellung für eine Verknüpfung zu ändern, wählen Sie die Verknüpfung aus und klicken Sie dann auf **Mit AD synchronisieren** oder **Desynchronisieren mit AD**.
   - Um die Auswirkungen einer Verknüpfung zu entfernen oder wiederherzustellen, wählen Sie die Verknüpfung aus und klicken Sie dann auf **Deaktivieren** bzw. **Aktivieren**.

Gehen Sie folgendermaßen vor, um Zugriffsvorlagenverknüpfungen anzuzeigen oder zu ändern, die die Berechtigungen für einen bestimmten Benutzer oder eine bestimmte Gruppe bestimmen:

1. Klicken Sie mit der rechten Maustaste auf den Benutzer oder die Gruppe und klicken Sie dann auf **Delegierte Rechte**.
2. Nehmen Sie im Dialogfeld **Delegierte Rechte** Folgendes vor:
   - Um eine neue Verknüpfung zu erstellen, klicken Sie auf **Hinzufügen** und befolgen dann die Anweisungen im Assistenten zum Delegieren der Kontrolle, um Berechtigungen für Benutzer oder Gruppen mit Hilfe einer Zugriffsvorlage festzulegen (Anweisungen finden Sie im Abschnitt Verfahren zum Anwenden einer Zugriffsvorlage weiter oben in diesem Dokument).
   - Um eine Verknüpfung zu löschen, wählen Sie sie aus der Liste aus und klicken Sie dann auf **Entfernen**.

- Um die Vererbungs- und Synchronisationseinstellungen für eine Verknüpfung anzuzeigen oder zu ändern, wählen Sie die Verknüpfung aus und klicken Sie dann auf **Anzeigen/ Bearbeiten**.
- Um die Synchronisationseinstellung für eine Verknüpfung zu ändern, wählen Sie die Verknüpfung aus und klicken Sie dann auf **Mit AD synchronisieren** oder **Desynchronisieren mit AD**.
- Um die Auswirkungen einer Verknüpfung zu entfernen oder wiederherzustellen, wählen Sie die Verknüpfung aus und klicken Sie dann auf **Deaktivieren** bzw. **Aktivieren**.

- Im Auslieferungszustand fuhrt das Dialogfeld **Quest One ActiveRoles-Sicherheit** zu einem Objekt alle Verknüpfungen auf, in denen die Berechtigungseinstellungen für dieses Objekt festgelegt werden, und zwar unabhängig davon, ob eine Verknüpfung für das Objekt selbst oder für einen Container oder eine verwaltete Einheit, in denen sich das Objekt befindet, angelegt wurde. Um die Anzeige der Liste zu ändern, deaktivieren Sie das Kontrollkästchen **Vererbung anzeigen**.
- In dem Dialogfeld **Quest One ActiveRoles-Sicherheit** können nur unmittelbare Verknüpfungen entfernt werden, das heißt, eine Verknüpfung kann nur dann entfernt werden, wenn sie in dem Objekt selbst angelegt worden ist (und nicht aus einem Container oder einer verwalteten Einheit übernommen wurde). Wenn Sie das Kontrollkästchen **Vererbung anzeigen** deaktivieren, werden nur direkte Verknüpfungen angezeigt. Sie können sie löschen, indem Sie auf **Entfernen** klicken.
- Im Dialogfeld der **Quest One ActiveRoles-Sicherheit** ist die Schaltflache **Entfernen** ausschließlich bei unmittelbaren Verknüpfungen verfügbar. Wenn Sie Verknüpfungen löschen müssen, ist es ratsam, dies mit Hilfe des Befehls **Verknüpfungen** für die Zugriffsvorlage oder mit Hilfe des Befehls **Delegierte Rechte** für den Trustee (Benutzer oder Gruppe) zu tun. Alternativ dazu können Sie eine Verknüpfung auch mit Hilfe von **Anzeigen/Bearbeiten** löschen: Wählen Sie die Verknüpfung aus und klicken Sie dann auf **Anzeigen/Bearbeiten**; klicken Sie dann auf **Eigenschaften** neben dem Feld **Zugriffsvorlage**; klicken Sie dann auf der Registerkarte **Verwaltung** auf **Verknüpfungen** und löschen Sie anschließend die Verknüpfung aus dem Dialogfeld **Verknüpfungen**.
- Im Dialogfeld der **Quest One ActiveRoles-Sicherheit** ist die Schaltflache **Mit AD synchronisieren** ausschließlich bei unmittelbaren Verknüpfungen verfügbar. Wenn Sie den Synchronisationsstatus einer Verknüpfung ändern müssen, ist es ratsam, dies mit Hilfe des Befehls **Verknüpfungen** für die Zugriffsvorlage oder mit Hilfe des Befehls **Delegierte Rechte** für den Trustee (Benutzer oder Gruppe) zu tun. Alternativ dazu können Sie den Synchronisationsstatus einer Verknüpfung auch mit Hilfe von **Anzeigen/Bearbeiten** ändern: Wählen Sie die Verknüpfung aus und klicken Sie dann auf **Anzeigen/ Bearbeiten**; aktivieren bzw. deaktivieren Sie dann auf der Registerkarte **Synchronisation** die Option **Berechtigungen an Active Directory weitergeben**.
- Durch Anklicken von **Anzeigen/Bearbeiten** wird das Dialogfeld **Eigenschaften** für die ausgewählte Verknüpfung angezeigt. Dieses Dialogfeld kann als Ausgangspunkt für die Verwaltung aller Elemente der Verknüpfung betrachtet werden. Ausgehend vom Dialogfeld **Eigenschaften** können Sie also auf die Eigenschaften des Verzeichnisobjekts, der Zugriffsvorlage und des Trustee zugreifen, der/die/das von der Verknüpfung abgedeckt werden, sowie die Einstellungen auf den Seiten **Vererbungsoptionen** und **Berechtigungsweitergabe** im Assistenten zum Delegieren der Kontrolle anzeigen und ändern und die Verknüpfung aktivieren oder deaktivieren.
- Die Zugriffsvorlagen können auch über die Registerkarten **Verknüpfungen (Links)** oder **ActiveRoles-Sicherheit** im Fenster der erweiterten Angaben verwaltet werden, dabei können dieselben Vorgange ausgeführt werden wie in den entsprechenden Dialogfeldern **Verknüpfungen (Links)** bzw. **Quest One ActiveRoles-Sicherheit**. Klicken Sie mit der rechten Maustaste auf eine Verknüpfung oder in einen leeren Bereich auf der Registerkarte und verwenden Sie Befehle aus dem Kontextmenü. Die Registerkarte **Verknüpfungen** wird angezeigt, wenn Sie eine Zugriffsvorlage auswählen. Ansonsten erscheint die Registerkarte **ActiveRoles-Sicherheit**. Um die erweiterte Detailanzeige anzuzeigen, aktivieren Sie **Erweiterte Detailansicht** im Menü **Ansicht** (siehe Erweiterter Bereich weiter oben in diesem Dokument).

Synchronisieren von Berechtigungen mit Active Directory

Quest One ActiveRoles bietet die Möglichkeit, die interne Sicherheit von Active Directory mithilfe ausgewählter, unter Verwendung von Zugriffsvorlagen angegebener Berechtigungen auf dem jeweils aktuellen Stand zu halten. Diese Option, die als *Weitergabe von Berechtigungen* bezeichnet wird, soll Benutzern und Anwendungen einheitliche Berechtigungen für Active Directory bereitstellen. Der normale Vorgang von Quest One ActiveRoles beruht nicht auf dieser Option.

Sie können die Option für die Weitergabe von Berechtigungen auf folgende Weisen festlegen:

- Bei der Anwendung von Zugriffsvorlagen können Sie das Kontrollkästchen **Berechtigungen an Active Directory weitergeben** im Assistenten zum Delegieren der Kontrolle aktivieren.
- Beim Verwalten von Zugriffsvorlagenverknüpfungen können Sie die Schaltfläche **Mit AD synchronisieren** in einem Fenster verwenden, in dem eine Liste von Verknüpfungen angezeigt wird, oder den Befehl **Mit AD synchronisieren** auf einer Registerkarte, auf der im erweiterten Bereich „Details" eine Liste von Verknüpfungen angezeigt wird, ausführen.

Angenommen Quest One ActiveRoles legt in Bezug auf eine Organisationseinheit bestimmte Berechtigungen fest, und Sie mochten diese mit Active Directory synchronisieren. Sie können diese Aufgabe wie folgt ausführen.

Klicken Sie zunächst mit der rechten Maustaste die Organisationseinheit an und dann mit links auf **Überwachung delegieren**, um das Fenster der **Quest One ActiveRoles-Sicherheit** aufzurufen.

Wählen Sie dann in der Liste **Zugriffsvorlagenverknüpfungen** die Verknüpfungen aus, die die zu synchronisierenden Berechtigungen definieren.

Klicken Sie zum Schluss auf die Schaltfläche **Mit AD synchronisieren**. In der Spalte **Mit interner Sicherheit synchronisieren** wird in der Aufstellung bei den Verknüpfungen, die synchronisiert werden, ein **Ja** angezeigt.

Nach Anklicken von **OK** legt Quest One ActiveRoles in Active Directory Berechtigungseintrage an, dank derer der Bevollmächtigte in Übereinstimmung mit den von Ihnen synchronisierten Zugriffsvorlagenverknupfungen in Active Directory über dieselben Rechte verfugt wie in der Quest One ActiveRoles-Umgebung.

Sie können die Synchronisierung von Berechtigungen jederzeit beenden, indem Sie auf die Schaltfläche **Desynchronisieren mit AD** klicken. Wenn Sie das tun, loscht Quest One ActiveRoles alle infolge der Synchronisierung angelegten Berechtigungseintrage in Active Directory.

Im **Quest One ActiveRoles-Sicherheit**sfenster steht die Schaltflache **Mit AD synchronisieren** ausschließlich bei unmittelbaren Verknüpfungen zur Verfugung. Wenn Sie Verknüpfungen synchronisieren möchten, sollten Sie sie mit dem Befehl **Verknüpfungen** für die Zugriffsvorlage verwalten.

Dieser Vorgang kann, wie folgt, auch mithilfe des Fensters der erweiterten Angaben ausgeführt werden:

1. Wahlen Sie die Organisationseinheit (OU) aus.
2. Wahlen Sie anschließend in der Registerkarte **ActiveRoles-Sicherheit** die Zugriffsvorlagenverknupfungen aus, in denen die Berechtigungen festgelegt werden, die synchronisiert werden sollen.
3. Klicken Sie diese Auswahl mit der rechten Maustaste an und anschließend mit links auf **Synchronisieren mit AD**.

Verwenden Sie den Befehl **Mit AD synchronisieren**, um den Synchronisierungsvorgang abzubrechen: Klicken Sie mit der rechten Maustaste auf die Verknüpfungen, die nicht mehr synchronisiert werden sollen, und klicken Sie dann auf **Desynchronisieren mit AD**.

In der Registerkarte **ActiveRoles-Sicherheit** ist der Befehl **Mit AD synchronisieren** ausschließlich bei unmittelbaren Verknüpfungen verfügbar. Wenn Sie Verknüpfungen synchronisieren möchten, sollten Sie sie mit der Registerkarte **Verknüpfungen** für die Zugriffsvorlage verwalten.

Verfahren zum Synchronisieren von Berechtigungen mit Active Directory

Quest One ActiveRoles bietet die Möglichkeit, die interne Sicherheit von Active Directory mithilfe ausgewählter, unter Verwendung von Zugriffsvorlagen angegebener Berechtigungseinstellungen auf dem jeweils aktuellen Stand zu halten. Diese Option, die als *Weitergabe von Berechtigungen* bezeichnet wird, soll Benutzern und Anwendungen einheitliche Berechtigungen für Active Directory bereitstellen. Im normalen Betrieb von Quest One ActiveRoles wird diese Option nicht verwendet.

Sie können die Option für die Weitergabe von Berechtigungen auf folgende Weisen festlegen:

- Aktivieren Sie beim Anwenden einer Zugriffsvorlage das Kontrollkästchen **Berechtigungen an Active Directory weitergeben** im Assistenten zum Delegieren der Kontrolle (siehe Verfahren zum Anwenden einer Zugriffsvorlage weiter oben in diesem Dokument).
- Verwenden Sie beim Verwalten von Zugriffsvorlagenverknüpfungen die Schaltfläche **Mit AD synchronisieren** in dem Dialogfeld, das eine Liste der Verknüpfungen anzeigt (siehe Verfahren zum Verwalten von Zugriffsvorlagenverknüpfungen weiter oben in diesem Dokument).

Als Beispiel können Sie die folgenden Anweisungen zur Festlegung der Berechtigungsverbreitungsoption für die Berechtigungseinstellungen verwenden, die durch Anwenden einer bestimmten Zugriffsvorlage auf eine Organisationseinheit definiert werden.

Gehen Sie folgendermaßen vor, um die Berechtigungseinstellungen für eine Organisationseinheit zu synchronisieren:

1. Klicken Sie mit der rechten Maustaste auf die Organisationseinheit und klicken Sie dann auf **Kontrolle delegieren**.
2. Wählen Sie im Dialogfeld **Quest One ActiveRoles-Sicherheit** die Verknüpfung „Zugriffsvorlage" aus, die die Berechtigungseinstellungen festlegt, die Sie mit Active Directory synchronisieren möchten, und klicken Sie dann auf **Mit AD synchronisieren**.
3. Klicken Sie auf **OK**, um das Dialogfeld **Quest One ActiveRoles-Sicherheit** zu schließen.

- Wenn Sie Berechtigungen mit Active Directory synchronisieren, erstellt Quest One ActiveRoles Berechtigungseinträge in Active Directory, sodass der Trustee anhand der Zugriffsvorlagenverknüpfungen, die Sie synchronisiert haben, in Active Directory über die gleichen Rechte verfügt wie in der Quest One ActiveRoles-Umgebung.
- Sie können die Synchronisierung von Berechtigungen jederzeit beenden, indem Sie auf die Schaltfläche **Desynchronisieren mit AD** klicken. Wenn Sie das tun, loscht Quest One ActiveRoles alle infolge der Synchronisierung angelegten Berechtigungseintrage in Active Directory.
- Sie können auch die Berechtigungsverbreitungsoption auf der Registerkarte **Verknüpfungen** oder **ActiveRoles-Sicherheit** in der erweiterten Detailanzeige verwalten, die es Ihnen ermöglicht, dieselben Aufgaben wie im Dialogfeld **Verknüpfungen** bzw. **Quest One ActiveRoles-Sicherheit** durchzuführen. Klicken Sie mit der rechten Maustaste auf die Verknüpfung, für die Sie die Berechtigungsverbreitungsoption festlegen möchten, und klicken Sie dann auf **Mit AD synchronisieren**,

um die Synchronisation zu starten, oder auf **Desynchronisieren mit AD**, um die Synchronisation zu stoppen. Die Registerkarte **Verknüpfungen** wird angezeigt, wenn Sie eine Zugriffsvorlage auswählen. Ansonsten erscheint die Registerkarte **ActiveRoles-Sicherheit**. Um die erweiterte Detailanzeige anzuzeigen, aktivieren Sie **Erweiterte Detailansicht** im Menü **Ansicht** (siehe Erweiterter Bereich weiter oben in diesem Dokument).

Verwalten von Berechtigungseinträgen in Active Directory

Auf der Registerkarte **Einheitliche Sicherheit** im erweiterten Bereich „Details" werden die einheitlichen Berechtigungseinträge von Active Directory für das in der Konsolenstruktur ausgewählte sicherbare Objekt (z. B. eine Organisationseinheit) aufgelistet.

Indem Sie Informationen in den Spalten **Typ** und **Quelle** auf der Registerkarte **Einheitliche Sicherheit** analysieren, können Sie erkennen, ob ein bestimmter Eintrag von Quest One ActiveRoles aus synchronisiert wird.

In der Spalte **Typ** sind die synchronisierten Einträge mit dem Symbol markiert. Dieses Symbol ändert sich zu , wenn die Synchronisierung des Eintrags ungültig oder nicht abgeschlossen ist. Wenn Sie beispielsweise einen synchronisierten Eintrag aus Active Directory löschen, erkennt Quest One ActiveRoles die Löschung und erstellt den Eintrag neu. Bis der Eintrag neu erstellt wird, ist er in der Spalte **Typ** mit dem Symbol markiert.

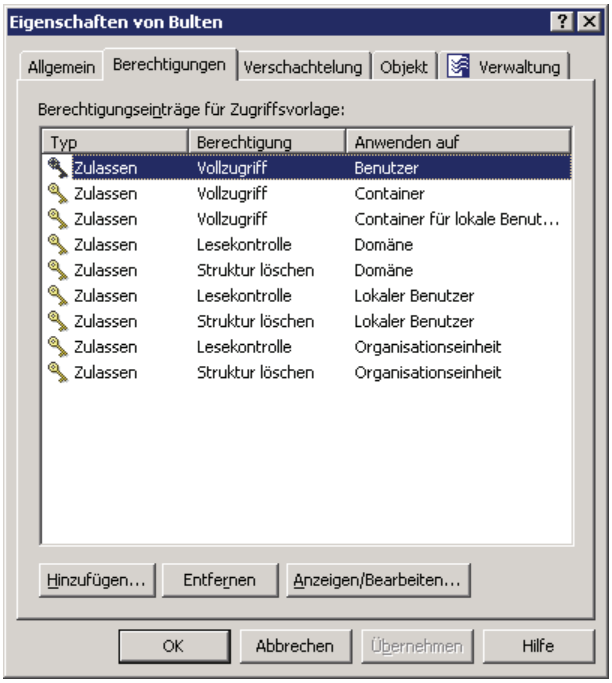
Für jeden synchronisierten Eintrag wird in der Spalte **Quelle** der Name der Zugriffsvorlage angezeigt, die die zu diesem Eintrag synchronisierten Berechtigungen definiert.

Auf der Registerkarte **Einheitliche Sicherheit** können Sie wie folgt Berechtigungseinträge verwalten: Klicken Sie mit der rechten Maustaste auf einen Eintrag und klicken Sie dann auf **Einheitliche Sicherheit bearbeiten**. Dann wird das Dialogfeld **Berechtigungen** angezeigt, in dem Sie Berechtigungseinträge von Active Directory für das ausgewählte sicherbare Objekt hinzufügen, entfernen und ändern können.

Hinzufügen, Ändern und Entfernen von Berechtigungen

Wenn Sie Berechtigungen in einer Zugriffsvorlage hinzufügen, entfernen oder ändern, werden automatisch Berechtigungseinstellungen für alle Objekte geändert, auf die die Zugriffsvorlage angewendet wird (mit denen sie verknüpft ist), einschließlich derjenigen, die aufgrund von Vererbung von der Zugriffsvorlage betroffen sind.

Um Berechtigungen in einer Zugriffsvorlage hinzuzufügen, zu entfernen oder zu ändern, zeigen Sie das Dialogfeld **Eigenschaften** für die Zugriffsvorlage an, und zeigen Sie dann die Registerkarte **Berechtigungen** an:



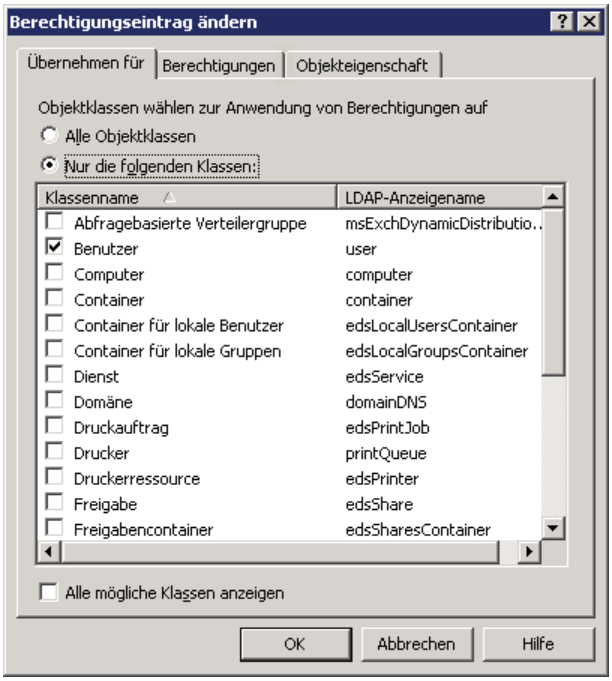
Auf der Registerkarte **Berechtigungen** werden Berechtigungseinträge aufgelistet, die in der Zugriffsvorlage definiert sind. Jeder Eintrag in der Liste schließt die folgenden Informationen ein:

- **Typ.** Gibt an, ob die Berechtigung den Zugriff zulässt oder verweigert.
- **Berechtigung.** Der Name der Berechtigung.
- **Anwenden auf.** Der Typ der Objekte, die der Berechtigung unterliegen.

Um eine neue Berechtigung hinzuzufügen, klicken Sie auf **Hinzufügen** und befolgen Sie die Anweisungen des Assistenten zum Hinzufügen von Berechtigungseinträgen wie unter Assistent zum Hinzufügen von Berechtigungseinträgen weiter oben in diesem Kapitel beschrieben.

Um Berechtigungen zu löschen, wählen Sie sie in der Liste **Berechtigungseinträge für Zugriffsvorlage** aus und klicken Sie dann auf **Entfernen**.

Um eine Berechtigung zu ändern, wählen Sie sie in der Liste **Berechtigungseinträge für Zugriffsvorlage** aus und klicken Sie dann auf **Anzeigen/Bearbeiten**. Damit wird das Dialogfeld **Berechtigungseintrag ändern** angezeigt, das der folgenden Abbildung ähnelt.



Auf den Registerkarten in diesem Dialogfeld können Sie die Berechtigungen nach Bedarf anpassen. Die Registerkarten sind identisch mit den Seiten im Assistenten zum Hinzufügen von Berechtigungseinträgen, die unter Assistent zum Hinzufügen von Berechtigungseinträgen weiter oben in diesem Kapitel beschrieben sind.

Verfahren zum Hinzufügen von Berechtigungen zu einer Zugriffsvorlage

Gehen Sie folgendermaßen vor, um einen Berechtigungseintrag zu einer Zugriffsvorlage hinzuzufügen:

1. Wählen Sie in der Konsolenstruktur unter **Configuration | Access Templates** den Ordner aus, der die Zugriffsvorlage enthält, die Sie ändern möchten.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf die Zugriffsvorlage und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf der Registerkarte **Berechtigungen** auf **Hinzufügen** und verwenden Sie dann den Assistenten zum Hinzufügen von Berechtigungseinträgen, um einen Berechtigungseintrag zu konfigurieren.

   Ausführlichere Anweisungen bezüglich des Hinzufügens eines Berechtigungseintrags zu einer Zugriffsvorlage finden Sie unter Verfahren zum Erstellen einer Zugriffsvorlage weiter oben in diesem Dokument.

- Auf der Registerkarte **Berechtigungen** werden die Berechtigungseinträge aufgelistet, die in der Zugriffsvorlage konfiguriert sind. Sie können die Registerkarte **Berechtigungen** verwenden, um Berechtigungseinträge zur Zugriffsvorlage hinzuzufügen, Berechtigungseinträge zu ändern oder Berechtigungseinträge aus der Zugriffsvorlage zu löschen.
- Wenn eine Zugriffsvorlage innerhalb von Quest One ActiveRoles angewandt wird, um die Berechtigungseinstellungen im Verzeichnis festzulegen, führen jegliche Änderungen an der Liste der Berechtigungseinträge in der Zugriffsvorlage dazu, dass die Berechtigungseinstellungen im Verzeichnis entsprechend geändert werden.
- Quest One ActiveRoles umfasst eine Reihe vordefinierter Zugriffsvorlagen. Die Liste der Berechtigungseinträge in einer vordefinierten Zugriffsvorlage kann nicht geändert werden. Wenn Sie Berechtigungseinträge zu einer vordefinierten Zugriffsvorlage hinzufügen, dort ändern oder aus der Zugriffsvorlage löschen müssen, erstellen Sie eine Kopie dieser Zugriffsvorlage und nehmen Sie dann die entsprechenden Änderungen an der Kopie vor. Eine weitere Option ist die Erstellung einer Zugriffsvorlage und die Verschachtelung der vordefinierten Zugriffsvorlage in der neu erstellten Zugriffsvorlage. Anweisungen finden Sie unter Verfahren zum Erstellen einer Zugriffsvorlage, Verfahren zum Kopieren einer Zugriffsvorlage und Verfahren zum Verwalten von verschachtelten Zugriffsvorlagen.

Verfahren zum Ändern von Berechtigungen in einer Zugriffsvorlage

Gehen Sie folgendermaßen vor, um einen Berechtigungseintrag in einer Zugriffsvorlage zu ändern:

1. Wählen Sie in der Konsolenstruktur unter **Configuration | Access Templates** den Ordner aus, der die Zugriffsvorlage enthält, die Sie ändern möchten.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf die Zugriffsvorlage und klicken Sie dann auf **Eigenschaften**.
3. Wählen Sie auf der Registerkarte **Berechtigungen** den Berechtigungseintrag, den Sie ändern möchten, klicken Sie auf **Anzeigen/Bearbeiten** und verwenden Sie dann die Registerkarten im Dialogfeld **Berechtigungseintrag ändern**, um Änderungen am Berechtigungseintrag vorzunehmen.

   Ausführlichere Anweisungen bezüglich der Anzeige oder Änderung eines Berechtigungseintrags in einer Zugriffsvorlage finden Sie unter Verfahren zum Erstellen einer Zugriffsvorlage weiter oben in diesem Dokument.

- Auf der Registerkarte **Berechtigungen** im Dialogfeld **Eigenschaften** werden die Berechtigungseinträge aufgelistet, die in der Zugriffsvorlage konfiguriert sind. Sie können die Registerkarte **Berechtigungen** verwenden, um Berechtigungseinträge zur Zugriffsvorlage hinzuzufügen, Berechtigungseinträge zu ändern oder Berechtigungseinträge aus der Zugriffsvorlage zu löschen.
- Die Optionen auf der Registerkarte **Berechtigungen** im Dialogfeld **Berechtigungseintrag ändern** sind schreibgeschützt. Wenn Sie eine andere Option für den Berechtigungseintrag auswählen müssen, müssen Sie den Berechtigungseintrag löschen und dann einen neuen Berechtigungseintrag mit der benötigten Option hinzufügen. Anweisungen finden Sie unter Verfahren zum Hinzufügen von Berechtigungen zu einer Zugriffsvorlage.
- Wenn eine Zugriffsvorlage innerhalb von Quest One ActiveRoles angewandt wird, um die Berechtigungseinstellungen im Verzeichnis festzulegen, führen jegliche Änderungen an der Liste der Berechtigungseinträge in der Zugriffsvorlage dazu, dass die Berechtigungseinstellungen im Verzeichnis entsprechend geändert werden.
- Quest One ActiveRoles umfasst eine Reihe vordefinierter Zugriffsvorlagen. Die Berechtigungseinträge in einer vordefinierten Zugriffsvorlage können nicht geändert werden. Wenn Sie einen Berechtigungseintrag in einer vordefinierten Zugriffsvorlage ändern müssen, erstellen Sie eine Kopie dieser Zugriffsvorlage und nehmen Sie dann die entsprechenden Änderungen an der Kopie vor. Anweisungen finden Sie unter Verfahren zum Kopieren einer Zugriffsvorlage.

Verfahren zum Entfernen von Berechtigungen aus einer Zugriffsvorlage

Gehen Sie folgendermaßen vor, um einen Berechtigungseintrag aus einer Zugriffsvorlage zu löschen:

1. Wählen Sie in der Konsolenstruktur unter **Configuration | Access Templates** den Ordner aus, der die Zugriffsvorlage enthält, die Sie ändern möchten.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf die Zugriffsvorlage und klicken Sie dann auf **Eigenschaften**.
3. Wählen Sie auf der Registerkarte **Berechtigungen** den Berechtigungseintrag aus, den Sie löschen möchten, klicken Sie dann auf **Entfernen** und klicken Sie anschließend auf **Ja**, um den Löschvorgang zu bestätigen.

- Auf der Registerkarte **Berechtigungen** werden die Berechtigungseinträge aufgelistet, die in der Zugriffsvorlage konfiguriert sind. Sie können die Registerkarte **Berechtigungen** verwenden, um Berechtigungseinträge zur Zugriffsvorlage hinzuzufügen, Berechtigungseinträge zu ändern oder Berechtigungseinträge aus der Zugriffsvorlage zu löschen.
- Wenn eine Zugriffsvorlage innerhalb von Quest One ActiveRoles angewandt wird, um die Berechtigungseinstellungen im Verzeichnis festzulegen, führen jegliche Änderungen an der Liste der Berechtigungseinträge in der Zugriffsvorlage dazu, dass die Berechtigungseinstellungen im Verzeichnis entsprechend geändert werden.
- Quest One ActiveRoles umfasst eine Reihe vordefinierter Zugriffsvorlagen. Berechtigungseinträge können nicht aus einer vordefinierten Zugriffsvorlage gelöscht werden. Wenn Sie die in einer vordefinierten Zugriffsvorlage enthaltene Liste der Berechtigungseinträge ändern müssen, erstellen Sie eine Kopie dieser Zugriffsvorlage und nehmen Sie dann die entsprechenden Änderungen an der Kopie vor. Anweisungen finden Sie unter Verfahren zum Kopieren einer Zugriffsvorlage.

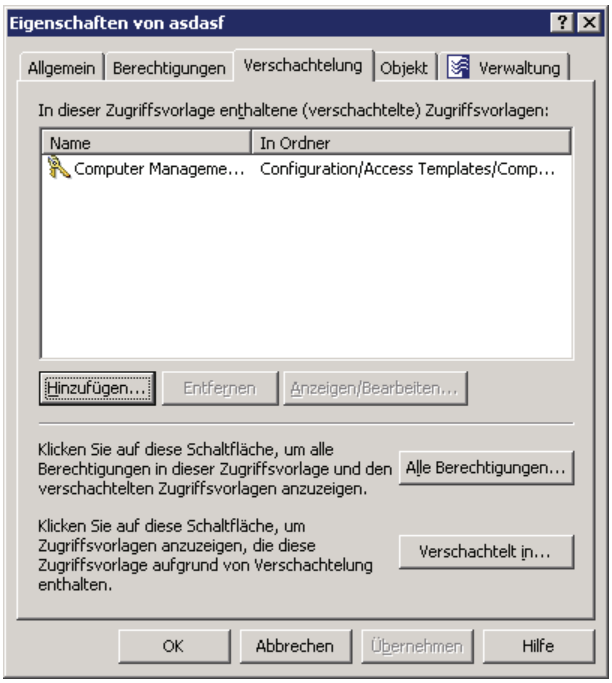
Schachteln von Zugriffsvorlagen

Quest One ActiveRoles ermöglicht das Definieren von Berechtigungen in einer Zugriffsvorlage durch Einschließen (Schachteln) anderer Zugriffsvorlagen. Dies reduziert die erforderliche Arbeit für das Erstellen einer neuen Zugriffsvorlage, die einer vorhandenen ähnelt. Statt eine vorhandene Vorlage durch Hinzufügen neuer Berechtigungen zu ändern, können Sie sie in eine neue Zugriffsvorlage schachteln.

Diese Funktion vereinfacht die Verwaltung von Zugriffsvorlagen durch Wiederverwenden der vorhandenen vordefinierten oder benutzerdefinierten Zugriffsvorlagen. Wenn Sie beispielsweise der vordefinierten Zugriffsvorlage für das Help Desk Berechtigungen hinzufügen möchten, können Sie eine neue Zugriffsvorlage erstellen, die Help Desk-Zugriffsvorlage in die neue Zugriffsvorlage schachteln und der neuen Zugriffsvorlage nach Bedarf Berechtigungen hinzufügen.

Um Zugriffsvorlagen in eine gegebene Zugriffsvorlage zu schachteln, verwenden Sie im Dialogfeld **Eigenschaften** für diese Zugriffsvorlage die Registerkarte **Verschachtelung**.

Auf der Registerkarte **Verschachtelung** werden alle Zugriffsvorlagen aufgelistet, die in die ausgewählte Zugriffsvorlage eingeschlossen (geschachtelt) sind, wie in der folgenden Abbildung:



Jeder Eintrag in der Liste stellt die folgenden Informationen bereit:

- **Name.** Den Namen der verschachtelten Zugriffsvorlage.
- **In Ordner.** Den Pfad zu dem Container, der die geschachtelte Zugriffsvorlage enthält.

Sie können die Liste auf der Registerkarte **Verschachtelung** mit Hilfe der Schaltflächen unter der Liste wie folgt verwalten:

- **Hinzufügen.** Klicken Sie auf diese Schaltfläche, um Zugriffsvorlagen auszuwählen, die Sie in die zu verwaltende Zugriffsvorlage schachteln möchten.
- **Entfernen.** Wählen Sie Zugriffsvorlagen in der Liste aus und klicken Sie auf diese Schaltfläche, um sie aus der zu verwaltenden Zugriffsvorlage zu entfernen.
- **Anzeigen/Bearbeiten.** Wählen Sie eine Zugriffsvorlage in der Liste aus und klicken Sie auf diese Schaltfläche, um die ausgewählte Zugriffsvorlage anzuzeigen oder zu ändern.

Über die Registerkarte **Verschachtelung** können Sie auch auf die folgenden Informationen zugreifen:

- **Alle Berechtigungen.** Zeigt alle Berechtigungen in der Zugriffsvorlage an, einschließlich derjenigen, die aus den geschachtelten Zugriffsvorlagen stammen.
- **Verschachtelt in.** Zeigt eine Liste der Zugriffsvorlagen an, in die die Zugriffsvorlage aufgrund der Schachtelung eingeschlossen ist.

Verfahren zum Verwalten von verschachtelten Zugriffsvorlagen

Gehen Sie folgendermaßen vor, um eine Zugriffsvorlage so zu konfigurieren, dass sie eine andere Zugriffsvorlage umfasst:

1. Wählen Sie in der Konsolenstruktur unter **Configuration | Access Templates** den Ordner aus, der die Zugriffsvorlage enthält, die Sie konfigurieren möchten.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf die Zugriffsvorlage und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf der Registerkarte **Verschachtelung** auf **Hinzufügen** und wählen Sie dann die Zugriffsvorlage aus, die in die Zugriffsvorlage aufgenommen werden soll, die Sie konfigurieren.

- Das Konfigurieren einer Zugriffsvorlage, so dass diese eine andere Zugriffsvorlage enthält, wird als *Verschachteln* bezeichnet. Die Registerkarte **Verschachtelung** enthält eine Liste der Zugriffsvorlagen, die in der Zugriffsvorlage verschachtelt sind. Sie können Zugriffsvorlagen zur Liste hinzufügen oder daraus entfernen.
- Die Verschachtelung einer Zugriffsvorlage in eine Ziel-Zugriffsvorlage führt zur Erweiterung der Liste der Berechtigungseinträge in der Ziel-Zugriffsvorlage um die Berechtigungseinträge der verschachtelten Zugriffsvorlage. Wenn also Zugriffsvorlage A in der Zugriffsvorlage B verschachtelt wird, werden alle in der Zugriffsvorlage A enthaltenen Berechtigungseinträge zur Liste der Berechtigungseinträge in Zugriffsvorlage B hinzugefügt.
- Sie können eine konsolidierte Liste der Berechtigungseinträge für die Zugriffsvorlage anzeigen: Klicken Sie auf der Registerkarte **Verschachtelung** auf **Alle Berechtigungen**. Die Liste umfasst sowohl die Berechtigungseinträge, die in der Zugriffsvorlage konfiguriert sind, als auch die Berechtigungseinträge, die sich in jeder Zugriffsvorlage befinden, die in der Zugriffsvorlage verschachtelt sind. Beachten Sie, dass auf der Registerkarte **Berechtigungen** im Dialogfeld **Eigenschaften** nur die Berechtigungseinträge aufgeführt sind, die in der Zugriffsvorlage konfiguriert sind. Die Berechtigungseinträge, die von anderen Zugriffsvorlagen aufgrund der Verschachtelung geerbt wurden, werden nicht auf der Registerkarte **Berechtigungen** aufgeführt.
- Sie können die Zugriffsvorlagen anzeigen, in denen die ausgewählte Zugriffsvorlage verschachtelt ist: Klicken Sie auf der Registerkarte **Verschachtelung** auf **Verschachtelt in**. Durch Doppelklicken auf Elemente in der Liste **Verschachtelt in** wird das Dialogfeld **Eigenschaften** für jede der Zugriffsvorlagen geöffnet, in der die ausgewählte Zugriffsvorlage verschachtelt ist.
- Die Verschachtelung ermöglicht Ihnen, die vorhandenen, vordefinierten oder benutzerdefinierten Zugriffsvorlagen wiederzuverwenden. Wenn Sie beispielsweise der vordefinierten Zugriffsvorlage für das **Help Desk** Berechtigungseinträge hinzufügen möchten, können Sie eine neue Zugriffsvorlage erstellen, die **Help Desk**-Zugriffsvorlage in die neu erstellte Zugriffsvorlage schachteln und der neuen Zugriffsvorlage nach Bedarf Berechtigungseinträge hinzufügen.

Kopieren einer Zugriffsvorlage

Mit der Quest One ActiveRoles-Konsole können Sie Kopien von Zugriffsvorlagen erstellen. Mit dieser Funktion können Sie vorhandene Zugriffsvorlagen wieder verwenden. Wenn Sie beispielsweise eine vordefinierte Zugriffsvorlage ändern möchten, können Sie sie kopieren und dann die Kopie nach Bedarf ändern.

Zum Erstellen einer Kopie einer Zugriffsvorlage klicken Sie mit der rechten Maustaste auf die Zugriffsvorlage und klicken Sie dann auf **Kopieren**. Dann wird der Assistent zum Kopieren des Objekts – Zugriffsvorlage geöffnet. Geben Sie einen Namen und eine Beschreibung für die Kopie ein und klicken Sie dann auf **Weiter**.

Auf der nächsten Seite des Assistenten wird eine Liste von Berechtigungseinträgen angezeigt. Standardmäßig schließt die Liste alle in der ursprünglichen Zugriffsvorlage definierten Einträge ein. Sie können die Liste auf die gleiche Weise wie auf der Registerkarte **Berechtigungen** im Dialogfeld **Eigenschaften** für eine Zugriffsvorlage ändern (siehe Hinzufügen, Ändern und Entfernen von Berechtigungen weiter oben in diesem Kapitel). Nach Abschluss der Arbeit mit der Liste der Berechtigungseinträge klicken Sie auf **Weiter** und dann auf **Fertig stellen**, um den Assistenten abzuschließen.

Verfahren zum Kopieren einer Zugriffsvorlage

So kopieren Sie eine Zugriffsvorlage:

1. Wählen Sie in der Konsolenstruktur unter **Configuration | Access Templates** den Ordner aus, der die Zugriffsvorlage enthält, die Sie kopieren möchten.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf die Zugriffsvorlage und klicken Sie dann auf **Kopieren**, um den Assistenten „Objekt kopieren – Zugriffsvorlage" zu starten.
3. Gehen Sie auf der ersten Seite des Assistenten wie folgt vor und klicken Sie dann auf **Weiter**:
   a) Geben Sie in das Feld **Name** den Namen für die neue Zugriffsvorlage ein.
   b) Geben Sie im Feld **Beschreibung** optionale Informationen über die neue Zugriffsvorlage ein.
4. Auf der zweiten Seite des Assistenten können Sie die Berechtigungseinträge hinzufügen, ändern und löschen, die aus der Original-Zugriffsvorlage kopiert wurden. Gehen Sie folgendermaßen vor und klicken Sie dann auf **Weiter**:
   - Um einen Berechtigungseintrag zur neuen Zugriffsvorlage hinzuzufügen, klicken Sie auf **Hinzufügen**.
   - Um einen Berechtigungseintrag für eine neue Zugriffsvorlage zu ändern, wählen Sie den Eintrag aus der Liste aus und klicken Sie dann auf **Anzeigen/Bearbeiten**.
   - Um einen Berechtigungseintrag aus der neuen Zugriffsvorlage zu löschen, wählen Sie den Eintrag aus der Liste aus und klicken Sie dann auf **Entfernen**.

   Ausführlichere Anweisungen bezüglich des Hinzufügens oder Änderns eines Berechtigungseintrags finden Sie unter Verfahren zum Erstellen einer Zugriffsvorlage weiter oben in diesem Dokument.
5. Klicken Sie auf **Fertig stellen**, um die Erstellung der neuen Zugriffsvorlage abzuschließen.

Exportieren und Importieren von Zugriffsvorlagen

Mit der Quest One ActiveRoles-Konsole können Sie Zugriffsvorlagen in eine XML-Datei exportieren und sie dann aus dieser Datei importieren, um eine andere Instanz von Quest One ActiveRoles aufzufüllen. Die Export- und Importvorgänge stellen eine Möglichkeit bereit, Zugriffsvorlagen von einer Testumgebung in eine Produktionsumgebung zu verschieben und umgekehrt.

Wenn Sie Zugriffsvorlagen exportieren und dann importieren, werden nur Berechtigungseinträge übertragen. Die Zugriffsvorlagenverknüpfungen sind nicht im Export-Import-Vorgang eingeschlossen. Daher müssen Sie sie nach Abschluss des Vorgangs manuell neu konfigurieren.

Um Zugriffsvorlagen zu exportieren, wählen Sie sie aus, klicken Sie mit der rechten Maustaste auf die Auswahl und wählen Sie dann **Alle Aufgaben | Exportieren**. Geben Sie im Dialogfeld **Objekte exportieren** die Datei an, in der Sie die Daten speichern möchten, und klicken Sie dann auf **Speichern**.

Zum Importieren von Zugriffsvorlagen klicken Sie mit der rechten Maustaste auf den Container, in dem Sie die Zugriffsvorlagen ablegen möchten, und klicken Sie dann auf **Importieren**. Wählen Sie im Dialogfeld **Verzeichnisobjekte importieren** die Datei aus, in die die Zugriffsvorlagen exportiert wurden, und klicken Sie dann auf **Öffnen**.

Umbenennen einer Zugriffsvorlage

Zum Umbenennen einer Zugriffsvorlage klicken Sie mit der rechten Maustaste auf die Zugriffsvorlage und klicken Sie dann auf **Umbenennen**. Geben Sie den neuen Namen ein und drücken Sie dann die Eingabetaste.

Das Umbenennen einer Zugriffsvorlage hat keine Auswirkungen auf ihre Verknüpfungen. Der Grund ist, dass auf Zugriffsvorlagen über unveränderliche Bezeichner statt über ihre Namen verwiesen wird.

Verfahren zum Umbenennen einer Zugriffsvorlage

So benennen Sie eine Zugriffsvorlage um:

1. Wählen Sie in der Konsolenstruktur unter **Configuration | Access Templates** den Ordner aus, der die Zugriffsvorlage enthält, die Sie umbenennen möchten.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf die Zugriffsvorlage und klicken Sie dann auf **Umbenennen**.
3. Geben Sie einen neuen Namen ein und drücken Sie dann die Eingabetaste.

- Wenn eine Zugriffsvorlage innerhalb von Quest One ActiveRoles angewandt wird, um die Berechtigungseinstellungen im Verzeichnis festzulegen, führt die Umbenennung der Zugriffsvorlage zu keinen Änderungen an den Berechtigungseinstellungen im Verzeichnis. Bei der Anwendung einer Zugriffsvorlage verweist Quest One ActiveRoles mit Hilfe einer internen Kennung und nicht mit Hilfe des Namens der Zugriffsvorlage auf die entsprechende Zugriffsvorlage.
- Quest One ActiveRoles umfasst eine Reihe vordefinierter Zugriffsvorlagen. Der Name einer vordefinierten Zugriffsvorlage kann nicht geändert werden. Wenn eine Zugriffsvorlage mit einem anderen Namen dieselben Berechtigungseinträge wie eine vordefinierte Zugriffsvorlage haben soll, erstellen Sie eine Kopie der vordefinierten Zugriffsvorlage und nehmen Sie dann die entsprechenden Änderungen an der Kopie vor. Eine weitere Option ist die Erstellung einer Zugriffsvorlage und die Verschachtelung der vordefinierten Zugriffsvorlage in der neu erstellten Zugriffsvorlage. Anweisungen finden Sie unter Verfahren zum Erstellen einer Zugriffsvorlage, Verfahren zum Kopieren einer Zugriffsvorlage und Verfahren zum Verwalten von verschachtelten Zugriffsvorlagen.

Löschen einer Zugriffsvorlage

Um eine Zugriffsvorlage zu löschen, müssen Sie zuerst wie folgt alle Verweise auf diese löschen:

- Löschen Sie die Verknüpfungen zur Zugriffsvorlage (siehe Verwalten von Zugriffsvorlagenverknüpfungen weiter oben in diesem Kapitel).
- Entfernen Sie die Zugriffsvorlage aus allen Zugriffsvorlagen, unter denen die Zugriffsvorlage verschachtelt ist (siehe Schachteln von Zugriffsvorlagen weiter oben in diesem Kapitel).

Dann können Sie den Löschvorgang wie folgt ausführen: Klicken Sie mit der rechten Maustaste auf die Zugriffsvorlage und klicken Sie dann auf **Löschen**.

Verfahren zum Löschen einer Zugriffsvorlage

So löschen Sie eine Zugriffsvorlage:

1. Wählen Sie in der Konsolenstruktur unter **Configuration | Access Templates** den Ordner aus, der die Zugriffsvorlage enthält, die Sie löschen möchten.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf die Zugriffsvorlage und klicken Sie dann auf **Löschen**.

- Wenn eine Zugriffsvorlage innerhalb von Quest One ActiveRoles angewandt (verknüpft) wird, um Berechtigungseinstellungen im Verzeichnis festzulegen, kann die Zugriffsvorlage nicht gelöscht werden. Sie können die Verknüpfungen anzeigen, an denen die Zugriffsvorlage beteiligt ist: Klicken Sie mit der rechten Maustaste auf Zugriffsvorlage und klicken Sie dann auf **Verknüpfungen**. Wenn Sie die Zugriffsvorlage löschen müssen, entfernen Sie zunächst alle Elemente aus der Liste **Verknüpfungen**. Anweisungen finden Sie unter Verfahren zum Verwalten von Zugriffsvorlagenverknüpfungen.
- Eine Zugriffsvorlage kann nicht gelöscht werden, wenn Sie in einer anderen Zugriffsvorlage verschachtelt ist. Sie können die Zugriffsvorlagen anzeigen, in denen die ausgewählte Zugriffsvorlage verschachtelt ist: Klicken Sie auf der Registerkarte **Verschachtelung** auf **Verschachtelt in**. Doppelklicken Sie auf ein Element in der Liste **Verschachtelt in**, um ein Dialogfeld zu öffnen, in dem Sie die Zugriffsvorlage aus der Verschachtelung entfernen können. Anweisungen finden Sie unter Verfahren zum Verwalten von verschachtelten Zugriffsvorlagen.
- Quest One ActiveRoles umfasst eine Reihe von vordefinierten Zugriffsvorlagen und eine Vielzahl von integrierten Zugriffsvorlagen. Weder vordefinierte Zugriffsvorlagen noch integrierte Zugriffsvorlagen können gelöscht werden.

Verwendungsbeispiele

In diesem Abschnitt werden Szenarien diskutiert, die Ihnen das Verstehen und die Verwendung der rollenbasierten Verwaltungsfunktionen erleichtern, die in Quest One ActiveRoles zur Verfügung stehen. Folgende Szenarien werden erörtert:

- Szenario 1: Implementieren eines Help Desk
- Szenario 2: Implementieren der Selbstverwaltung

Szenario 1: Implementieren eines Help Desk

In diesem Szenario wird gezeigt, wie Sie mit Hilfe einer Zugriffsvorlage einem Help Desk-Service die Ausführung täglicher Vorgänge für Benutzerkonten ermöglichen, z.B. das Zurücksetzen von Kennwörtern, Anzeigen von Benutzereigenschaften sowie das Sperren und Entsperren von Benutzerkonten.

In dem Szenario kommt auch eine Gruppe vor, die Help Desk-Operatoren enthalten soll. Die Zugriffsvorlage wird angewendet, sodass die Gruppe als Trustee ausgewählt wird und die Help Desk-Operatoren somit Administratorrechte erhalten. Nach der Vorbereitung der Zugriffsvorlage und der Gruppe können Sie eine Help Desk-Verwaltung im Unternehmen implementieren.

Angenommen, Sie möchten das Help Desk autorisieren, Benutzerkonten in der Organisationseinheit **Vertrieb** zu verwalten. Führen Sie zum Implementieren dieses Szenarios die folgenden Schritte aus:

1. Bereiten Sie die Zugriffsvorlage **Help Desk** vor, in der die Berechtigungen für Help Desk-Operatoren in Bezug auf Benutzerkonten definiert sind.
2. Erstellen Sie die Gruppe **Help Desk**, die die Help Desk-Operatoren enthalten soll, und füllen Sie sie auf.
3. Wenden Sie die Zugriffsvorlage **Help Desk** auf die Organisationseinheit **Vertrieb** an und wählen Sie dabei die Gruppe **Help Desk** als Trustee aus.

Als Ergebnis dieser Schritte wird jedes Mitglied der Gruppe **Help Desk** dazu autorisiert, Verwaltungsaufgaben für Benutzerkonten in der Organisationseinheit **Vertrieb** auszuführen. Die Zugriffsvorlage **Help Desk** bestimmt den Bereich dieser Aufgaben.

In den folgenden Abschnitten werden alle diesen Schritte ausführlich beschrieben.

Schritt 1: Vorbereiten einer Zugriffsvorlage für das Help Desk

Für dieses Szenario können Sie die vordefinierte Zugriffsvorlage **Users – Help Desk** im Ordner **Configuration/Access Templates/Active Directory** verwenden. Die Zugriffsvorlage **Users – Help Desk** gibt die notwendigen Berechtigungen zum Zurücksetzen von Benutzerkennwörtern, zum Entsperren von Benutzerkonten sowie zum Anzeigen ihrer Eigenschaften an.

Um Berechtigungen zur Zugriffsvorlage **Users – Help Desk** hinzuzufügen oder aus ihr zu entfernen, müssen Sie zuerst eine Kopie dieser Zugriffsvorlage erstellen und diese Kopie dann ändern und anwenden.

Für dieses Szenario wird angenommen, dass Sie die vordefinierte Zugriffsvorlage **Users – Help Desk** anwenden.

Schritt 2: Erstellen einer Gruppe für das Help Desk

Um eine Gruppe zu erstellen, klicken Sie mit der rechten Maustaste auf eine Organisationseinheit in der Konsolenstruktur, wählen Sie dann **Neu | Gruppe** aus und befolgen Sie anschließend die Anweisungen des Assistenten „Neues Objekt – Gruppe". Der Assistent schließt die Seite ein, auf der Sie der gerade erstellten Gruppe Mitglieder (Help Desk-Operatoren) hinzufügen können.

Schrittweise Anleitungen bezüglich der Erstellung von Gruppen finden Sie im Abschnitt „Verfahren zum Erstellen einer Gruppe" im *Quest One ActiveRoles Benutzerhandbuch* oder in der Quest One ActiveRoles-Hilfe.

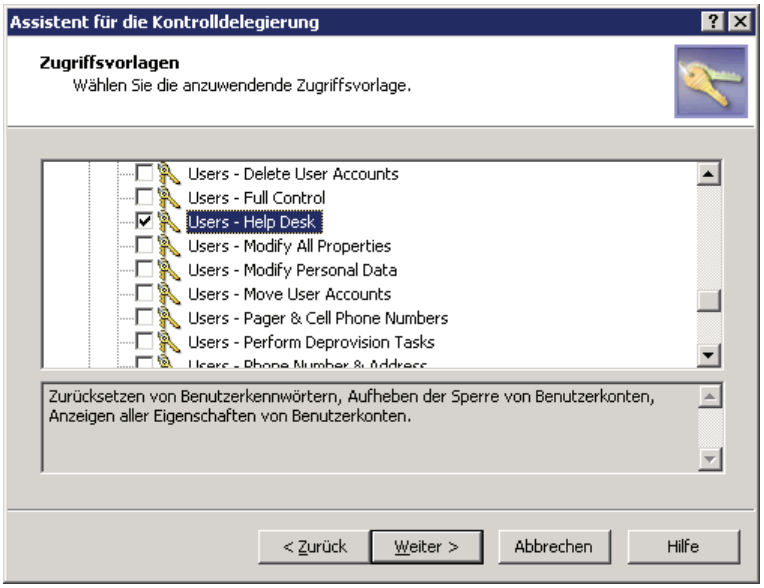
Schritt 3: Anwenden der Zugriffsvorlage für das Help Desk

Sie können die Zugriffsvorlage anwenden, indem Sie den Assistenten zum Delegieren der Kontrolle verwenden:

Starten Sie zunächst den Assistenten wie folgt für die Organisationseinheit **Vertrieb**: Klicken Sie mit der rechten Maustaste auf die Organisationseinheit, klicken Sie auf **Kontrolle delegieren** und klicken Sie dann im Fenster **Quest One ActiveRoles-Sicherheit** auf die Schaltfläche **Hinzufügen**.

Fügen Sie dann auf der Seite **Benutzer oder Gruppen** des Assistenten die Gruppe **Help Desk** zu der Liste hinzu.

Erweitern Sie dann auf der Seite **Zugriffsvorlagen** des Assistenten die Option **Zugriffsvorlagen | Active Directory** und aktivieren Sie das Kontrollkästchen neben **Users – Help Desk** (siehe folgende Abbildung).


Assistent für die Kontrolldelegierung
Zugriffsvorlagen
Wählen Sie die anzuwendende Zugriffsvorlage.
Users - Delete User Accounts
Users - Full Control
Users - Help Desk
Users - Modify All Properties
Users - Modify Personal Data
Users - Move User Accounts
Users - Pager & Cell Phone Numbers
Users - Perform Deprovision Tasks
Zurücksetzen von Benutzerkennwörtern, Aufheben der Sperre von Benutzerkonten, Anzeigen aller Eigenschaften von Benutzerkonten.
< Zurück
Weiter >
Abbrechen
Hilfe

Klicken Sie auf **Weiter**, und akzeptieren Sie die Standardeinstellungen des Assistenten. Klicken Sie auf der Abschlussseite auf **Fertig stellen**. Klicken Sie zum Schluss auf **OK**, um das Fenster **Quest One ActiveRoles-Sicherheit** zu schließen.

Ausführlichere Informationen über den Assistenten zum Delegieren der Kontrolle finden Sie unter Anwenden von Zugriffsvorlagen weiter oben in diesem Kapitel.

Szenario 2: Implementieren der Selbstverwaltung

In diesem Szenario wird die Verwendung einer Zugriffsvorlage gezeigt, die Benutzern das Ändern bestimmter Teile ihrer persönlichen Daten in Active Directory ermöglicht.

Das Web-Interface von Quest One ActiveRoles stellt die Seite für die Selbstverwaltung bereit, über die Benutzerkonten verwaltet werden können. Auf der Seite werden den Benutzern ihre persönlichen Daten angezeigt, z.B. Vor- und Nachnamen, Adressdaten, Telefonnummern und andere Daten. Standardmäßig sind Benutzer des Web-Interface nur zum Anzeigen ihrer persönlichen Daten autorisiert. Damit die Benutzer ihre persönlichen Daten auch ändern können, müssen Sie ihnen zusätzliche Berechtigungen erteilen.

Angenommen, Sie möchten die Benutzer in der Organisationseinheit **Vertrieb** zur Ausführung von Selbstverwaltung autorisieren. Führen Sie zum Implementieren dieses Szenarios die folgenden Schritte aus:

1. Bereiten Sie die Zugriffsvorlage **Self-Administration** vor, in der die geeigneten Berechtigungen in Bezug auf Benutzerkonten definiert sind.
2. Wenden Sie die Zugriffsvorlage **Self-Administration** auf die Organisationseinheit **Vertrieb** an und wählen Sie dabei das Objekt **Selbst** als Trustee aus.

Nach Ausführung dieser Schritte sind Benutzer aus der Organisationseinheit **Vertrieb** dazu autorisiert, Selbstverwaltungsaufgaben für ihre persönlichen Konten auszuführen. Die Zugriffsvorlage **Self-Administration** bestimmt, welche Daten die Benutzer ändern können. Benutzer können mit Hilfe der Selbstverwaltungsseite ihre persönlichen Daten verwalten. Weitere Informationen über die Selbstverwaltungsseite finden Sie im *Quest One ActiveRoles Web-Interface – Benutzerhandbuch*.

In den folgenden Abschnitten werden die Schritte in diesem Szenario detailliert erörtert.

Schritt 1: Vorbereiten einer Zugriffsvorlage für die Selbstverwaltung

Für dieses Szenario können Sie die vordefinierte Zugriffsvorlage **Self-Service – My Account Management** im Ordner **Configuration/Access Templates/User Self-management** verwenden. Diese Zugriffsvorlage gibt die notwendigen Berechtigungen zum Anzeigen grundlegender Benutzereigenschaften und zum Ändern von Telefonnummern an.

Um Berechtigungen zur Zugriffsvorlage **Self - My Account Management** hinzuzufügen oder aus ihr zu entfernen, müssen Sie zuerst eine Kopie dieser Zugriffsvorlage erstellen und diese Kopie dann ändern und anwenden.

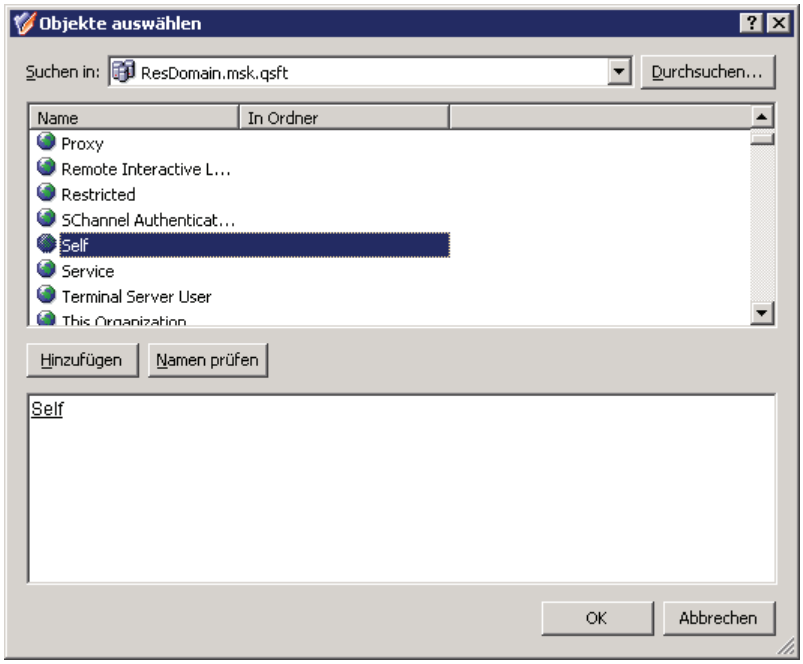
Für dieses Szenario wird angenommen, dass Sie die vordefinierte Zugriffsvorlage **Self - Account Management** anwenden.

Schritt 2: Anwenden der Zugriffsvorlage für die Selbstverwaltung

Sie können die Zugriffsvorlage anwenden, indem Sie den Assistenten zum Delegieren der Kontrolle verwenden:

Starten Sie zunächst den Assistenten wie folgt für die Organisationseinheit **Vertrieb**: Klicken Sie mit der rechten Maustaste auf die Organisationseinheit, klicken Sie auf **Kontrolle delegieren** und klicken Sie dann im Fenster **Quest One ActiveRoles-Sicherheit** auf die Schaltfläche **Hinzufügen**.

Klicken Sie dann auf der Seite **Benutzer oder Gruppen** des Assistenten auf die Schaltfläche **Hinzufügen**. Wählen Sie im Fenster **Objekte auswählen** das Objekt **Self** (siehe folgende Abbildung), klicken Sie dann auf **Hinzufügen** und anschließend auf **OK**.



Erweitern Sie dann auf der Seite **Zugriffsvorlagen** des Assistenten die Option **Zugriffsvorlagen | Benutzer-Selbstverwaltung** und aktivieren Sie das Kontrollkästchen neben **Selbst - Kontoverwaltung**.

Klicken Sie auf **Weiter**, und akzeptieren Sie die Standardeinstellungen des Assistenten. Klicken Sie auf der Abschlussseite auf **Fertig stellen**. Klicken Sie zum Schluss auf **OK**, um das Fenster **Quest One ActiveRoles-Sicherheit** zu schließen.

Ausführlichere Informationen über den Assistenten zum Delegieren der Kontrolle finden Sie unter Anwenden von Zugriffsvorlagen weiter oben in diesem Kapitel.

Überlegungen bezüglich der Bereitstellung

Quest One ActiveRoles nutzt die rollenbasierte Delegation für die Zuordnung administrativer Berechtigungen. Dieses Modell hat den Vorteil, dass eine Rolle einmal erstellt und dann an mehrere Benutzergruppen, die dieser Rolle entsprechen, delegiert werden kann. Wenn eine Änderung erforderlich ist, hat die Aktualisierung der Rolle Auswirkungen auf alle, denen diese Rolle zugeordnet ist. Diese Rollen werden als „Zugriffsvorlagen" bezeichnet.

Beim Delegieren von Rollen mittels Quest One ActiveRoles sollten Sie folgende Regeln berücksichtigen:

- Quest One ActiveRoles-Administratoren (ActiveRoles-Admins) haben Vollzugriff auf das gesamte System. Ihnen kann nirgendwo innerhalb von Quest One ActiveRoles der Zugriff verwehrt werden. Alle anderen Benutzer haben zunächst gar keine Berechtigungen. Ihnen werden dann nach und nach die entsprechenden Berechtigungen hinzugefügt.
- Berechtigungen sind kumulativ, und eine explizite Zurückweisung hat Vorrang vor einer expliziten Erlaubnis. Eine explizite Erlaubnis hat Vorrang vor einer vererbten Zurückweisung.
- Das Berechtigungsmodell sollte so einfach wie möglich gestaltet werden. Manchmal bedeutet dies, den Benutzern alle Lese-/Schreibberechtigungen einzuräumen und die Möglichkeit zum Schreiben einiger weniger Felder zurückzuweisen.
- Verwenden Sie nicht die standardmäßigen (integrierten) Zugriffsvorlagen, da diese nicht geändert werden können. Kopieren Sie statt dessen diese Zugriffsvorlagen und verschieben Sie sie in einen neuen Container. Auf diese Weise befinden sich alle von Ihnen verwendeten Zugriffsvorlagen innerhalb einer bestimmten Struktur.

Es gibt drei grundlegende Berechtigungstypen, die zu einer Zugriffsvorlage hinzugefügt werden können:

- Der erste ist der *Objektzugriff*. Mit diesem Berechtigungstyp können Sie Berechtigungen festlegen, die ein Objekt als Ganzes betreffen. Beispiel: Verschieben; Auflisten; Deprovisionieren - alle dies sind Objektberechtigungen.
- Der zweite ist der *Objekteigenschaftszugriff*. Dieser Berechtigungstyp wird verwendet, um den Zugriff auf einzelne Attribute eines Objekts wie etwa die Beschreibung, samAccountName oder homeFolder des Objekts zuzugreifen. Mit diesem Berechtigungstyp können Sie granuläre Rechte über ein Objekt delegieren. Dass die Rechte, die delegiert werden können, granulär sein können, bedeutet jedoch nicht, dass sie dies auch sein müssen. Wenn beispielsweise ein Help Desk Operator eine Vielzahl an Benutzereigenschaften verwalten können muss, ist es sinnvoller, Lese-/Schreibberechtigungen für alle Eigenschaften zu delegieren, da es sich hierbei um nur einen Berechtigungseintrag handelt, anstatt die Lese-/Schreibrechte für jedes einzelne Attribut zu delegieren, da jedes Attribut seinen eigenen Berechtigungseintrag erfordern würde.
- Der dritte Berechtigungstyp ist die *Erstellung/Löschung von untergeordneten Objekten*. Mit diesem Berechtigungstyp können Sie Berechtigungen für das Erstellen oder Löschen von Objekten festlegen. Um beispielsweise eine Zugriffsvorlage einzurichten, die die Erstellung von Benutzern ermöglicht, sollten Sie einen Berechtigungseintrag hinzufügen, der für die Objektklassen „Organisationseinheit" und „Containerobjekt" gilt und die Berechtigung „Untergeordnete Objekte erstellen" für die Objektklasse „Benutzer" enthält.

Im folgenden Abschnitt ist eine beispielhafte Reihe von Berechtigungen aufgeführt, die für bestimmte Delegationsszenarien erforderlich sind:

- Delegation der Administration einer Organisationseinheit
- Delegieren der Gruppenadministration

Delegation der Administration einer Organisationseinheit

In der folgenden Tabelle ist beispielhaft eine Reihe von Berechtigungseinträgen für ein Szenario zur Delegation der Administration von Organisationseinheiten aufgeführt:

OBJEKTKLASSE	BERECHTIGUNGSTYP	ATTRIBUT ODER BERECHTIGUNG
Domäne	Objektzugriff	„Auflisten" ermöglichen
Domäne	Objekteigenschaftszugriff	„Alle Eigenschaften lesen" ermöglichen
Domäne	Objekteigenschaftszugriff	„LDAP-Server schreiben" ermöglichen (Berechtigung zur Änderung des aktiven Domänencontrollers)
Organisationseinheit	Objektzugriff	„Auflisten" ermöglichen
Organisationseinheit	Objekteigenschaftszugriff	„Alle Eigenschaften lesen" ermöglichen
Organisationseinheit	„Untergeordnete Objekte erstellen/löschen" ermöglichen	„Benutzer erstellen/löschen" ermöglichen
Benutzer	Objektzugriff	„Auflisten" ermöglichen
Benutzer	Objekteigenschaftszugriff	„Alle Eigenschaften lesen/schreiben" ermöglichen
Benutzer	Objekteigenschaftszugriff	„Mitarbeiter-ID schreiben" verweigern

Diese Berechtigungseinträge haben verschiedene wichtige Eigenschaften:

- Sie ermöglichen den Zugriff auf die Objektklassen „Domäne" und „Organisationseinheit". Dies ist erforderlich, da ein delegierter Administrator ohne den Zugriff auf die Domäne und die Organisationseinheiten nicht die darunter befindlichen Benutzer sehen kann. Dieser Zugriff sollte immer die Berechtigungen „Auflisten" und „Alle Eigenschaften lesen" umfassen.
- Er ermöglicht dem delegierten Administrator die Erstellung und Löschung von Benutzerobjekten. Diese Berechtigung gilt für die Objektklasse „Organisationseinheit".
- Sie ermöglicht dem delegierten Administrator, Benutzer zu sehen (Auflisten) und jegliche Eigenschaften mit Ausnahme der Mitarbeiter-ID zu ändern.

Delegieren der Gruppenadministration

In der folgenden Tabelle ist beispielhaft eine Reihe von Berechtigungseinträgen für ein Szenario zur Delegation der Administration von Gruppen aufgeführt:

OBJEKTKLASSE	BERECHTIGUNGSTYP	ATTRIBUT ODER BERECHTIGUNG
Domäne	Objektzugriff	„Auflisten" ermöglichen
Domäne	Objekteigenschaftszugriff	„Alle Eigenschaften lesen" ermöglichen
Domäne	Objekteigenschaftszugriff	„LDAP-Server schreiben" ermöglichen (Berechtigung zur Änderung des aktiven Domänencontrollers)
Organisationseinheit	Objektzugriff	„Auflisten" ermöglichen
Organisationseinheit	Objekteigenschaftszugriff	„Alle Eigenschaften lesen" ermöglichen
Organisationseinheit	„Untergeordnete Objekte erstellen/löschen" ermöglichen	„Gruppen erstellen/löschen" ermöglichen
Gruppe	Objektzugriff	„Auflisten" ermöglichen
Gruppe	Objekteigenschaftszugriff	„Alle Eigenschaften lesen" ermöglichen
Gruppe	Objekteigenschaftszugriff	„Mitglieder schreiben" ermöglichen
Benutzer	Objektzugriff	„Auflisten" ermöglichen
Benutzer	Objekteigenschaftszugriff	„Alle Eigenschaften lesen" ermöglichen

Diese Berechtigungseinträge haben verschiedene wichtige Eigenschaften:

- Sie ermöglichen den Zugriff auf die Objektklassen „Domäne" und „Organisationseinheit". Dies ist erforderlich, da ein delegierter Administrator ohne den Zugriff auf die Domäne und die Organisationseinheiten nicht die darunter befindlichen Gruppen und Benutzer sehen kann. Dieser Zugriff sollte immer die Berechtigungen „Auflisten" und „Alle Eigenschaften lesen" umfassen.
- Er ermöglicht dem delegierten Administrator die Erstellung und Löschung von Gruppenobjekten. Diese Berechtigung gilt für die Objektklasse „Organisationseinheit".
- Die Berechtigung ermöglicht einem delegierten Administrator, Gruppen zu sehen (Auflisten), jegliche Eigenschaften einer Gruppe anzuzeigen (Alle Eigenschaften lesen) und Mitglieder zu einer Gruppe hinzuzufügen bzw. aus ihr zu entfernen (Mitglieder schreiben).
- Sie ermöglicht dem delegierten Administrator, Benutzer anzuzeigen (Auflisten) und jegliche Eigenschaften eines Benutzers einzusehen (Alle Eigenschaften lesen). Dies ist erforderlich, damit ein delegierter Administrator Benutzer zu einer Gruppe hinzufügen kann.

Delegation in einer funktionalen Umgebung im Vergleich zu einer gehosteten Umgebung

Damit Ihr Delegationsmodell korrekt funktioniert, müssen Sie festlegen, ob Sie über eine funktionale oder gehostete Umgebung verfügen.

Delegieren in einer funktionalen Umgebung

In einer funktionalen Umgebung gibt es eine separate Administratorengruppe für jede Funktion. So gibt es möglicherweise eine Gruppe für die Verwaltung von Benutzern, ein Help Desk, Domänenadministratoren und Exchange-Administratoren. Bei einer funktionalen Umgebung müssen Sie jeder Funktion eine bestimmte Rolle zuweisen. Diese Rollen überschreiten normalerweise die Grenzen der Organisationseinheiten, daher wird die Delegation üblicherweise auf der untersten Domänenebene durchgeführt. Ein Delegationsmodell für dieses Szenario würde in etwa wie folgt aussehen:

STANDORT/VORLAGE	BERECHTIGUNG	DELEGIEREN (TRUSTEE)
Domäne/Alle Objekte lesen	• Alle Objekte - Auflisten • All Objects – Read All Properties • Domäne - LDAP-Servereigenschaft schreiben (Berechtigung zur Änderung des aktiven Domänencontrollers)	Authentifizierte Benutzer
Domäne/Benutzer-Admin	• Benutzerobjekte - Vollzugriff • Organisationseinheit - Benutzerobjekte erstellen/ löschen	Gruppe „Benutzeradministratoren“
Domäne/Gruppen-Admin	• Gruppenobjekte - Vollzugriff • Organisationseinheit - Gruppenobjekte erstellen/ löschen	Gruppe „Gruppenadministratoren“

Delegieren in einer gehosteten Umgebung

In einer gehosteten Umgebung gibt es eine Administratorengruppe oder mehrere Administratorengruppen, die für jede Organisationseinheit der obersten Ebene verantwortlich ist. In diesem Fall möchten die Administratoren möglicherweise nicht, dass andere einsehen können, was in der Struktur ihrer Organisationseinheit vor sich geht. Quest One ActiveRoles kann dies ganz einfach realisieren. Da mit Ausnahme der Quest One ActiveRoles-Administratoren niemand über Standard-Berechtigungen verfügt, könnte das Delegationsmodell in etwa wie folgt aussehen:

STANDORT/VORLAGE	BERECHTIGUNG	DELEGIEREN (TRUSTEE)
Domäne/Domäne lesen	• Domänen - Auflisten • Domänen - Alle Eigenschaften lesen • Domäne - LDAP-Servereigenschaft schreiben	Authentifizierte Benutzer
Organisationseinheit der obersten Ebene/ Organisationseinheit-Admin	• Alle Objekte - Auflisten • Alle Objekte - Alle Eigenschaften lesen • Organisationseinheit - Benutzer-/Gruppenobjekte erstellen/löschen • Benutzerobjekte - Vollzugriff • Gruppenobjekte - Vollzugriff	Organisationseinheit-Admin

Bei diesem Delegationsmodell kann jeder die Domäne einsehen und den für die Verwaltung verwendeten Domänencontroller ändern. Darunter können jedoch nur die Organisationseinheit-Administratoren deren zugeordnete Organisationseinheit einsehen. Dies vermeidet, dass Administratoren irgendetwas außerhalb ihres Zuständigkeitsbereichs einsehen oder verwalten können.

Ein Delegationsmodell würde höchstwahrscheinlich Funktionen für Beides umfassen. So können Sie beispielsweise über eine gehostete Umgebung verfügen, in der jede Unternehmenseinheit für ihre eigene Active Directory-Verwaltung zuständig ist und ein zentrales Help Desk grundlegende Aufgaben zur Benutzer- und Gruppenverwaltung durchführt.

Zuletzt steht das Problem der Synchronisation der Berechtigungen für Active Directory. Obwohl Quest One ActiveRoles Ihnen die Durchführung dieser Aufgabe ermöglicht, empfiehlt es sich aus folgenden Gründen, alle Berechtigungen innerhalb von Quest One ActiveRoles zu belassen:

- Dies schützt Ihr Active Directory. Directory-fähige Anwendungen können dahingehend verändert werden, dass Sie den Quest One ActiveRoles ADSI Provider nutzen, was einen granulären Zugriff nur auf wirklich benötigten Daten und Bereiche ermöglicht. Dies erhöht den Schutz vor bösartiger Software, die Daten in Active Directory beschädigen könnte.
- Das alles gewährleistet die Integrität der Verzeichnisse. Indem Sie alle Administratoren zwingen, Quest One ActiveRoles zu nutzen, gewährleisten Sie, dass alle Richtlinien wie etwa Benennungsstandards korrekt umgesetzt werden.
- Dies ergibt ein umfassendes Auditing-Bild. Indem alle Anwendungen und Administratoren die Benutzeroberflächen von Quest One ActiveRoles verwenden, gewährleisten Sie, dass der Report Data Collector von Quest One ActiveRoles alle Aktionen erfassen kann, die in dem Verzeichnis durchgeführt werden - und zwar bis hin zur Attributebene.

5

Regelbasierte automatische Bereitstellung und Deprovisionierung

- Richtlinienobjekte
- Verwaltungsaufgaben für Richtlinienobjekte
- Konfigurationsaufgaben für Richtlinien
- Überlegungen bezüglich der Bereitstellung
- Überprüfen der Richtlinieneinhaltung
- Deprovisionieren von Benutzern oder Gruppen
- Wiederherstellen von deprovisionierten Benutzern oder Gruppen
- Richtlinie zur Vermeidung einer Containerlöschung
- Richtlinienerweiterungen

Richtlinienobjekte

Active Directory ermöglicht eine sehr granuläre Delegierung der Kontrolle. Die Möglichkeit, den Zugriff einzuschränken, reicht jedoch möglicherweise nicht aus.

Viele Aktivitäten bei der Verzeichnisverwaltung folgen einem vordefinierten Workflow. Bei diesem Workflow wird eine Reihe von Aufgaben in einer bestimmten Reihenfolge ausgeführt. Administratoren und andere Mitarbeiter müssen wiederholt fast identische Aufgaben ausführen. Einige Beispiele: Erstellen von Benutzerkonten, Zurücksetzen von Kennwörtern, Deaktivieren inaktiver Benutzerkonten, Durchsetzen von Namenskonventionen für Benutzer.

Quest One ActiveRoles bietet eine richtlinienbasierte Verwaltungslösung, die die Anforderungen heutiger Unternehmen erfüllt. Die Durchsetzung administrativer Richtlinien in Quest One ActiveRoles reduziert die Arbeitslast für die Verwaltung erheblich, verbessert die Netzwerksicherheit und stellt unternehmensweite Konsistenz sicher. Durch die Automatisierung des Verwaltungsworkflows wird die Zeit für die Ausführung von Aufgaben deutlich reduziert, und einige Aufgaben können völlig eliminiert werden. Außerdem wird die Fehleranfälligkeit minimiert, die Notwendigkeit von Nacharbeiten wird reduziert, und zusammengehörige Aktionen werden in einem einzelnen Batch kombiniert.

Mit Quest One ActiveRoles können Sie angeben, was bei jeder Änderung, Erstellung oder Löschung von Verzeichnisobjekten wann und wie geändert werden muss. Außerdem können Sie Quest One ActiveRoles so konfigurieren, dass nur Datenänderungen akzeptiert werden, die bestimmte Formatierungsanforderungen erfüllen. So können Sie die im Verzeichnis gespeicherten Daten besser steuern.

Wenn Sie beispielsweise ein Benutzerkonto für einen neuen Mitarbeiter erstellen, kann Quest One ActiveRoles automatisch Informationen aus einer Datenbank der Personalabteilung abrufen, sie in den Eigenschaften des Benutzerkontos als Standardinformationen verwenden, einen Stammordner und eine Stammfreigabe erstellen und das neue Konto den notwendigen Gruppen hinzufügen. Außerdem kann das Programm ein Exchange-Postfach erstellen und es den relevanten Verteilungslisten hinzufügen. Das gesamte Vorgehen bedeutet eine einzige Aufgabe, während es ohne Quest One ActiveRoles zehn oder mehr Aufgaben darstellen kann.

Dank der Möglichkeit, administrative Richtlinien durchzusetzen und Verwaltungsworkflows zu automatisieren, spart Quest One ActiveRoles nicht nur Zeit, sondern erhält auch Netzwerkobjekte in einem konsistenten Zustand im Verhältnis zu den einzelnen definierten Richtlinien. Dies betrifft wichtige Fragen der Sicherheit, Verwendbarkeit und Integrität, die für die Verwaltung von Netzwerkobjektdaten von zentraler Bedeutung sind.

In Quest One ActiveRoles werden administrative Richtlinien mit Hilfe von Richtlinienobjekten definiert. Dabei handelt es sich um Sammlungen von Richtlinien. Richtlinienobjekte definieren das Verhalten des Systems bei der Erstellung, Änderung oder Löschung von Verzeichnisobjekten.

Sie können ein Richtlinienobjekt erstellen, das beliebig viele unterschiedliche Richtlinien enthält, wie beispielsweise eine Formatüberprüfung, Generierungsregeln für die Werte von Objektattributen, Skripts zur Ergänzung administrativer Vorgänge, die automatische Erstellung von Benutzerpostfächern auf vorgegebenen Exchange-Servern, eine automatische Erstellung von Stammordnern und Stammfreigaben für Benutzer sowie Neuzuordnung eines Objekts zu einem angegebenen Container, wenn es bestimmte Kriterien erfüllt.

Quest One ActiveRoles stellt umfangreiche Automatisierungsfunktionen für administrative Prozesse bereit. Richtlinienobjekte können anpassbare Skripts vor oder nach der Ausführung eines beliebigen spezifischen Tasks ausführen, und mehrere Tasks können in einen Vorgang kombiniert werden. Diese Funktionalität reduziert den Zeitaufwand für Verwaltungsaufgaben wesentlich und minimiert Fehler.

Mit Hilfe von Richtlinienobjekten automatisiert Quest One ActiveRoles die Aufgaben der Bereitstellung für Benutzer, verringert so Ihre Arbeitslast für die Verwaltung und ermöglicht es, neuen Benutzern schneller die benötigten Ressourcen bereitzustellen. Das Programm automatisiert außerdem auch die erneute Bereitstellung und die Deprovisionierung. Wenn der Zugriff eines Benutzers geändert oder entfernt werden muss, werden Aktualisierungen in Active Directory, Exchange und Windows also automatisch vorgenommen. Dies reduziert die Arbeitslast für die Verwaltung und ermöglicht Benutzern eine schnellere, größere Produktivität.

Um Ihnen das Konfigurieren und Anwenden von Richtlinienobjekten zu erleichtern, werden sie in zwei Kategorien eingeteilt:

- **Bereitstellungsrichtlinienobjekte** Mit diesen Objekten werden Bereitstellungsregeln angegeben. Dazu gehören Regeln zur Auffüllung und Überprüfung von Verzeichnisdaten, zur Erstellung von Ressourcen wie Stammordnern und Postfächern sowie zur Bereitstellung eines Ressourcenzugriffs.
- **Deprovisionsrichtlinienobjekte** Mit diesen Objekten werden Deprovisionierungsregeln angegeben. Dazu gehören Regeln zum Entfernen von Benutzerkonten und E-Mail-Konten, Stammordnern, Sicherheits- und Verteilungslisten sowie des Anwendungszugriffs in Reaktion auf Anforderungen zur Deprovisionierung von Benutzern oder Gruppen.

Sie können beliebig viele Richtlinienobjekte in jeder der beiden Kategorien erstellen und anwenden.

Bereitstellungsrichtlinienobjekte

Bereitstellungsrichtlinienobjekte ermöglichen die Konfiguration und Anwendung der folgenden Richtlinien.

RICHTLINIE	BESCHREIBUNG
Erzeugung von Benutzeranmeldenamen	Diese Richtlinie erzeugt einen Benutzeranmeldenamen (Prä-Windows 2000) für ein neu erstelltes Benutzerkonto. Sie können sie für Folgendes konfigurieren: • Hinzufügen einer Eindeutigkeitszahl zum generierten Anmeldenamen • Anwenden mehrerer Regeln für das Generieren eines Anmeldenamens • Ermöglichen, dass während des Benutzererstellungsprozesses ein Anmeldename manuell angegeben wird Indem Sie diese Optionen kombinieren, können Sie sicherstellen, dass der Benutzer-Anmeldename (Prä-Windows 2000) eindeutig ist. Dies ist eine Schemaanforderung in Active Directory.
E-Mail-Aliaserzeugung	Diese Richtlinie stellt sicher, dass für neu erstellte Benutzerkonten die geeigneten E-Mail-Aliasnamen eingerichtet sind. Sie können sie für die Generierung von Aliasen konfigurieren, denen Folgendes zugrunde liegt: • Vorher ausgewählte Benutzereigenschaften, wie Vor- und Nachnamen • Eine benutzerdefinierte Auswahl von Eigenschaften, nicht auf Benutzereigenschaften eingeschränkt Mit dieser Richtlinie kann jeder Alias eindeutig gemacht werden, indem ihm eine Eindeutigkeitszahl hinzugefügt wird.

Automatische Bereitstellung des Exchange-Postfachs	Mit dieser Richtlinie wird sichergestellt, dass Benutzerpostfächer in geeigneten Postfachspeichern oder Datenbanken erstellt werden. Sie können sie für Folgendes konfigurieren: • Bestimmen der Postfachspeicher oder Datenbanken, in denen die Erstellung von Postfächern zulässig ist • Anwenden einer Regel für das Verteilen von Postfächern auf mehrere Speicher oder Datenbanken Mit dieser Richtlinie können Sie Postfächer im Kreisverfahren verteilen oder jeweils im Speicher oder in der Datenbank mit den wenigsten Postfächern ablegen.
Automatische Bereitstellung der Gruppenmitgliedschaft	Diese Richtlinie stellt sicher, dass Benutzerkonten den geeigneten Gruppen angehören. Sie können sie für Folgendes konfigurieren: • Hinzufügen von Benutzerkonten zu bestimmten Gruppen • Entfernen von Benutzerkonten aus bestimmten Gruppen Sie können Gruppen auswählen und Kriterien einrichten. Die Richtlinie fügt ein Benutzerkonto zu den gewählten Gruppen hinzu oder entfernt es aus diesen, je nachdem, ob das Benutzerkonto die angegebenen Kriterien erfüllt. Die Richtlinie kann ebenfalls auf andere Verzeichnisobjekte als Benutzerkonten angewendet werden.
Stammordner AutoProvisioning	Diese Richtlinie führt Bereitstellungsaktionen durch, die zur Zuweisung von Stammordnern und Stammfreigaben zu Benutzerkonten erforderlich sind. Sie können sie für Folgendes konfigurieren: • Erstellen von Stammordnern für neu erstellte Benutzerkonten • Umbenennen von Stammordnern beim Umbenennen von Benutzerkonten Sie können den Server angeben, auf dem Stammordner und freigaben erstellt werden sollen, Namenskonventionen für Stammordner und freigaben bestimmen sowie Zugriffsrechte für die neu erstellten Stammordner und freigaben konfigurieren.
Erzeugung und Validierung von Eigenschaften	Diese Richtlinie erzeugt und validiert Verzeichnisdaten wie Benutzereigenschaften. Sie können sie für Folgendes konfigurieren: • Auffüllen des Verzeichnisses mit Standarddaten • Ausführen von Datengültigkeitsprüfungen bei Verzeichnisaktualisierungen Sie können angeben, wie die Richtlinie Verzeichnisdaten standardmäßig generieren soll und welche Überprüfungskriterien angewendet werden müssen, um sicherzustellen, dass die Verzeichnisdaten Ihren Unternehmensstandards entsprechen.
Skriptausführung	Diese Richtlinie führt auf Anfrage ein Skript aus, um bestimmte Vorgänge wie die Erstellung oder Aktualisierung von Benutzerkonten durchzuführen. Mit Skripts können Sie folgende Vorgänge ausführen: • Auslösen zusätzlicher Aktionen für die Benutzerbereitstellung • Regulierung von Datenformaten und anforderungen • Automatisierung von Verwaltungsaufgaben Sie können ein benutzerdefiniertes Skript mit einem administrativen Vorgang verknüpfen und dem Skript die Kontrolle geben, wenn der Vorgang angefordert wird oder nachdem er abgeschlossen wurde.

Deprovisionsrichtlinienobjekte

Richtlinienobjekte zur Deprovisionierung ermöglichen die Konfiguration und Anwendung der folgenden Richtlinien.

POLICY	BESCHREIBUNG
Benutzerkonto-Deprovisionierung	Diese Richtlinie ändert bei der Deprovisionierung für einen Benutzer das Benutzerkonto, damit sich der Benutzer nicht anmelden kann. Sie können diese Richtlinie für Folgendes konfigurieren: • Benutzerkonto deaktivieren • Kennwort des Benutzers in einen willkürlichen Wert ändern • Festlegen der Anmeldenamen des Benutzers auf zufällige Werte • Benutzerkonto umbenennen Sie können auch Kontoeigenschaften auswählen und diese Richtlinie so konfigurieren, dass sie sie bei der Verarbeitung einer Rücknahmeanforderung für eine Bereitstellung aktualisiert.
Entfernung der Gruppenmitgliedschaft	Diese Richtlinie entfernt bei der Deprovisionierung für einen Benutzer das Benutzerkonto aus Gruppen. Sie können diese Richtlinie so konfigurieren, dass das Konto aus Sicherheitsgruppen, Mail-aktivierten Gruppen oder beiden entfernt wird. Bei dieser Richtlinie werden sowohl Verteilergruppen als auch E-Mail-fähige Sicherheitsgruppen zusammen als E-Mail-fähige Gruppen bezeichnet. Sie können auch die Gruppen auswählen, aus denen diese Richtlinie das Benutzerkonto nicht entfernen soll, oder die Richtlinie so konfigurieren, dass sie das Benutzerkonto aus keiner Sicherheitsgruppe und keiner E-Mail-fähigen Gruppe entfernt.
Benutzerkonto-Verschiebung	Diese Richtlinie verschiebt bei der Deprovisionierung für einen Benutzer das Benutzerkonto an einen anderen Ort. Sie können die Organisationseinheit wählen, in die die Richtlinie das Konto verschieben soll. Sie können die Richtlinie auch so konfigurieren, dass sie bei der Deprovisionierung für einen Benutzer die Benutzerkonten nicht verschiebt.
Exchange-Postfach-Deprovisionierung	Diese Richtlinie nimmt bei der Deprovisionierung für einen Benutzer notwendige Änderungen vor, um die Bereitstellung von Microsoft Exchange-Ressourcen für diesen Benutzer zurückzunehmen. Sie können diese Richtlinie für Folgendes konfigurieren: • Ausblenden des Postfachs aus der globalen Adressliste • Senden von Unzustellbarkeitsberichten (NDR) verhindern • Vorgesetztem des Benutzers Vollzugriff auf das Postfach des Benutzers gewähren • Ausgewählten Benutzern oder Gruppen Vollzugriff auf das Postfach des Benutzers gewähren • Verweigern der Nachrichtenweiterleitung an alternative Empfänger • Weiterleiten aller eingehenden Nachrichten an den Vorgesetzten des Benutzers
Stammordner-Deprovisionierung	Diese Richtlinie nimmt bei der Deprovisionierung für einen Benutzer notwendige Änderungen vor, damit der Benutzer nicht mehr auf seinen Stammordner zugreifen kann. Sie können diese Richtlinie für Folgendes konfigurieren: • Benutzerberechtigungen für Basisordner entfernen • Gewähren von Lesezugriff auf den Stammordner des Benutzers an den Vorgesetzten des Benutzers • Gewähren von Lesezugriff auf den Stammordner des Benutzers für ausgewählte Benutzer oder Gruppen • Festlegen eines ausgewählten Benutzers oder einer ausgewählten Gruppe als Besitzer des Stammordners des Benutzers • Den Basisordner beim Löschen des Benutzerkontos löschen

Permanentes Löschen des Benutzerkontos	Bei der Deprovisionierung für einen Benutzer plant diese Richtlinie die Löschung des Benutzerkontos. Sie können die Anzahl der Tage (Wartezeitraum) festlegen, bevor das Konto gelöscht wird. Eine andere Option ist das Löschen der deprovisionierten Benutzerkonten (sofortiges Verschieben in den Active Directory-Papierkorb). Sie können diese Richtlinie auch so konfigurieren, dass deprovisionierte Benutzerkonten nicht automatisch gelöscht werden.
Gruppenobjekt-Deprovisionierung	Diese Richtlinie nimmt bei der Deprovisionierung einer Gruppe Änderungen am Gruppenobjekt in Active Directory vor, um die Verwendung der Gruppe zu vermeiden. Sie können diese Richtlinie für Folgendes konfigurieren: • Gruppe in der globalen Adressliste (GAL) ausblenden • Gruppentyp von „Sicherheit" in „Verteilung" ändern • Gruppe umbenennen • Mitglieder aus der Gruppe entfernen • Jegliche andere Eigenschaften des Gruppenobjekts ändern oder löschen
Gruppenobjekt-Verschiebung	Bei der Deprovisionierung einer Gruppe verschiebt diese Richtlinie das Gruppenobjekt in einen anderen Container in Active Directory. Sie können die Organisationseinheit wählen, in die die Richtlinie das Gruppenobjekt verschieben soll.
Dauerhaftes Löschen des Gruppenobjekts	Bei der Deprovisionierung einer Gruppe plant diese Richtlinie die Löschung des Gruppenobjekts in Active Directory. Sie können die Anzahl der Tage (Aufbewahrungsdauer) festlegen, bevor die Gruppe gelöscht wird. Eine andere Option ist das Löschen der deprovisionierten Gruppen (sofortiges Verschieben in den Active Directory-Papierkorb). Sie können diese Richtlinie auch so konfigurieren, dass deprovisionierte Gruppen nicht automatisch gelöscht werden.
Benachrichtigungsverteilung	Im Verlauf eines Deprovisionierungsvorgangs sendet diese Richtlinie eine Benachrichtigungsmeldung an die angegebenen E-Mail-Empfänger. Sie können sowohl den Betreff als auch den Text der Nachricht anpassen.
Berichtsverteilung	Nach Abschluss eines Deprovisionierungsvorgangs sendet diese Richtlinie einen Bericht an die angegebenen E-Mail-Empfänger. Der Bericht umfasst eine Liste der während des Deprovisionierungsvorgangs durchgeführten Aktionen sowie die Details der Deprovisionierungsaktivität. Sie können den Betreff der E-Mail-Nachricht mit dem Bericht anpassen. Sie können die Richtlinie ebenfalls so konfigurieren, dass der Bericht nur dann gesendet wird, wenn im Verlauf eines Deprovisionierungsvorgangs Fehler aufgetreten sind.
Skriptausführung	Im Verlauf des Deprovisionierungsvorgangs führt diese Richtlinie das von Ihnen angegebene Skript aus. Mithilfe eines Skripts können Sie benutzerdefinierte Aktionen für die Deprovisionierung implementieren.

Funktionsweise von Richtlinienobjekten

Ein Richtlinienobjekt ist eine Sammlung administrativer Richtlinien, mit denen die durchzusetzenden Geschäftsregeln angegeben werden. Ein Richtlinienobjekt schließt gespeicherte Richtlinienprozeduren und Angaben von Ereignissen ein, die die jeweilige Prozedur aktivieren.

Ein Richtlinienobjekt ordnet seinen Richtlinienprozeduren spezifische Ereignisse zu, bei denen es sich um integrierte Prozeduren oder benutzerdefinierte Skripts handeln kann. Dies ermöglicht das einfache Definieren von Richtlinieneinschränkungen, das Implementieren komplexer Überprüfungskriterien, das Synchronisieren verschiedener Datenquellen und das Ausführen einer Reihe von Verwaltungstasks in einem einzelnen Batch.

Quest One ActiveRoles setzt Geschäftsregeln durch Verknüpfen von Richtlinienobjekten mit Folgendem um:

- Administrative Ansichten (Quest One ActiveRoles Verwaltete Einheiten)
- Active Directory-Container (Organisationseinheiten)
- Einzelne Verzeichnisobjekte (Blattobjekte), z.B. Benutzer- oder Gruppenobjekte

Indem Sie auswählen, wo ein Richtlinienobjekt verknüpft wird, bestimmen Sie den Gültigkeitsbereich der Richtlinie. Wenn Sie ein Richtlinienobjekt beispielsweise mit einem Container verknüpfen, unterliegen alle Objekte in dem Container und in seinen Untercontainern normalerweise dem Richtlinienobjekt.

Sie können unterschiedliche Richtlinienobjekte mit unterschiedlichen Containern verknüpfen, um containerspezifische Richtlinien einzurichten. Dies müssen Sie möglicherweise in Situationen ausführen, in denen für jede Organisationseinheit ein eigener Exchange-Server zum Speichern von Postfächern oder ein eigener Dateiserver zum Speichern von Stammordnern verwendet wird.

Sie können ein Richtlinienobjekt auch mit einem Blattobjekt verknüpfen, z.B. mit einem Benutzerobjekt. Betrachten Sie beispielsweise eine Richtlinie, die Änderungen an Gruppenmitgliedschaften beim Kopieren eines bestimmten Benutzerobjekts verbietet.

Richtlinienobjekte definieren das Verhalten des Systems bei der Erstellung, Änderung, Verschiebung oder Löschung von Verzeichnisobjekten im Gültigkeitsbereich der Richtlinie. Richtlinien werden ungeachtet der Administratorrechte des Benutzers durchgesetzt, der die Verwaltungsaufgabe ausführt. Beachten Sie, dass aktive administrative Richtlinien auch für Benutzer mit Administratorrechten für Quest One ActiveRoles selbst durchgesetzt werden.

Verwaltungsaufgaben für Richtlinienobjekte

In diesem Abschnitt wird die Verwaltung von Richtlinienobjekten mit der Quest One ActiveRoles-Konsole vorgestellt. Folgende Themen werden erörtert:

- Erstellen eines Richtlinienobjekts
- Hinzufügen, Ändern und Entfernen von Richtlinien
- Anwenden von Richtlinienobjekten
- Verwalten des Richtlinienbereichs
- Kopieren eines Richtlinienobjekts
- Umbenennen eines Richtlinienobjekts
- Exportieren und Importieren von Richtlinienobjekten
- Löschen eines Richtlinienobjekts

Erstellen eines Richtlinienobjekts

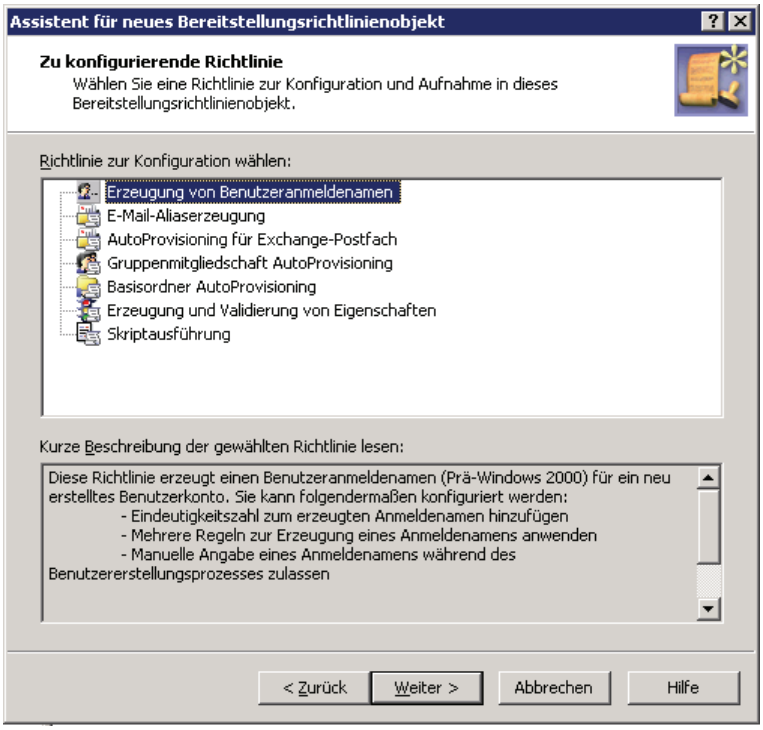
Die Quest One ActiveRoles-Konsole stellt separate Assistenten für die Erstellung von Richtlinienobjekten in jeder Kategorie (Bereitstellung und Deprovisionierung) bereit. Sie können die Assistenten vom Container **Administration** aus starten. Dieser befindet sich in der Konsolenstruktur unter **Configuration/Policies**:

- Klicken Sie zum Konfigurieren von Bereitstellungsrichtlinien in der Konsolenstruktur mit der rechten Maustaste auf **Administration** und wählen Sie dann **Neu | Richtlinie wird bereitgestellt** aus.
- Klicken Sie zum Konfigurieren von Deprovisionierungsrichtlinien in der Konsolenstruktur mit der rechten Maustaste auf **Administration** und wählen Sie dann **Neu | Deprovisionierungsrichtlinie** aus.

Für die Verwaltung einer großen Anzahl von Richtlinienobjekten sollten Sie wie folgt Container erstellen, die nur angegebene Richtlinienobjekte enthalten, damit Sie sie leicht finden können: Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Administration** und wählen Sie dann **Neu | Container**. Verwenden Sie dann die Assistenten, um Richtlinienobjekte in diesem Container zu erstellen: Klicken Sie mit der rechten Maustaste auf den Container und klicken Sie dann auf **Neu | Bereitstellungsrichtlinie** oder **Neu | Deprovisionierungsrichtlinie**.

Klicken Sie auf der Seite **Willkommen** des Assistenten auf **Weiter**. Geben Sie dann auf der Seite **Name und Beschreibung** einen Namen und eine Beschreibung für das neue Richtlinienobjekt ein. Auf der Quest One ActiveRoles-Konsole werden im Bereich „Details" in der Liste der Richtlinienobjekte der Name und die Beschreibung angezeigt.

Klicken Sie auf **Next (Weiter)**, um den Vorgang fortzusetzen. Nun wird eine Seite angezeigt, auf der Sie die zu konfigurierende Richtlinie auswählen können. Die Liste der Richtlinien hängt davon ab, ob Sie ein Richtlinienobjekt für die Bereitstellung oder eines für die Deprovisionierung erstellen. Beispielsweise ähnelt die Liste der Bereitstellungsrichtlinien der folgenden Abbildung.


Assistent für neues Bereitstellungsrichtlinienobjekt
Zu konfigurierende Richtlinie
Wählen Sie eine Richtlinie zur Konfiguration und Aufnahme in dieses Bereitstellungsrichtlinienobjekt.
Richtlinie zur Konfiguration wählen:
Erzeugung von Benutzeranmeldenamen
E-Mail-Aliaserzeugung
AutoProvisioning für Exchange-Postfach
Gruppenmitgliedschaft AutoProvisioning
Basisordner AutoProvisioning
Erzeugung und Validierung von Eigenschaften
Skriptausführung
Kurze Beschreibung der gewählten Richtlinie lesen:
Diese Richtlinie erzeugt einen Benutzeranmeldenamen (Prä-Windows 2000) für ein neu erstelltes Benutzerkonto. Sie kann folgendermaßen konfiguriert werden:
- Eindeutigkeitszahl zum erzeugten Anmeldenamen hinzufügen
- Mehrere Regeln zur Erzeugung eines Anmeldenamens anwenden
- Manuelle Angabe eines Anmeldenamens während des Benutzererstellungsprozesses zulassen
< Zurück
Weiter >
Abbrechen
Hilfe

Wählen Sie auf der Seite **Zu konfigurierende Richtlinie** den Typ der Richtlinie aus, die Sie dem Richtlinienobjekt hinzufügen möchten. Nach Auswahl des Typs wird seine Beschreibung im unteren Feld angezeigt.

Klicken Sie auf **Weiter**, um die Richtlinie zu konfigurieren. Die Schritte für das Konfigurieren einer Richtlinie hängen vom Richtlinientyp ab. Anweisungen bezüglich der Konfiguration von Richtlinien finden Sie unter Konfigurationsaufgaben für Richtlinien weiter unten in diesem Kapitel.

Nach Abschluss der Richtlinienkonfiguration wird eine Seite des Assistenten angezeigt, auf der Sie den Gültigkeitsbereich der Richtlinie angeben können: Sie können eine Liste der Container oder verwalteten Einheiten zusammenstellen, für die die Richtlinie durchgesetzt werden soll. Dieser Schritt ist optional, da Sie den Richtlinienbereich nach der Erstellung des Richtlinienobjekts konfigurieren können (siehe Anwenden von Richtlinienobjekten weiter unten in diesem Kapitel).

Klicken Sie auf **Weiter** und klicken Sie dann auf **Fertig stellen**, um den Assistenten abzuschließen. Nun wird das neue Richtlinienobjekt erstellt.

Verfahren zur Erstellung eines Richtlinienobjekts

So erstellen Sie ein Richtlinienobjekt:

1. Wählen Sie in der Konsolenstruktur unter **Configuration | Policies | Administration** den Ordner aus, zu dem Sie das Richtlinienobjekt hinzufügen möchten.

   *Gehen Sie folgendermaßen vor, um einen neuen Ordner zu erstellen: Klicken Sie mit der rechten Maustaste auf **Administration** und wählen Sie dann **Neu | Container**. Auf die gleiche Weise können Sie einen Unterordner in einem Ordner erstellen: Klicken Sie mit der rechten Maustaste auf den Ordner und wählen Sie **Neu | Container**.*

2. Klicken Sie mit der rechten Maustaste auf den Ordner, zeigen Sie auf **Neu** und klicken Sie dann auf **Bereitstellungsrichtlinie** oder **Deprovisionierungsrichtlinie**.
3. Klicken Sie auf der Seite Willkommen des Assistenten auf **Weiter**.
4. Gehen Sie auf der Seite **Name und Beschreibung** wie nachfolgend beschrieben vor und klicken Sie dann auf **Weiter**:

   a) Geben Sie in das Feld **Name** den Namen des Richtlinienobjekts ein.

   b) Geben Sie unter **Beschreibung** nach Bedarf Informationen über das Richtlinienobjekt ein.

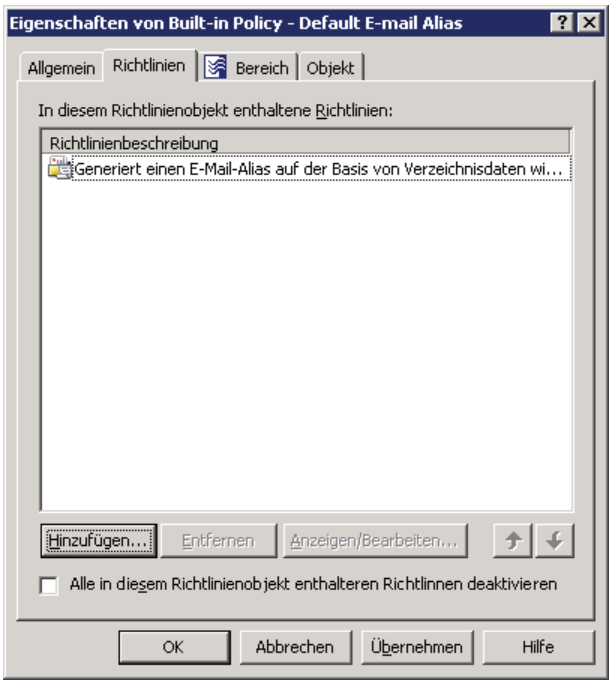
5. Wählen Sie auf der Seite **Zu konfigurierende Richtlinie** einen Richtlinientyp aus und klicken Sie dann auf **Weiter**, um Richtlinieneinstellungen zu konfigurieren.
6. Auf der Seite **Richtlinie erzwingen** können Sie die Objekte angeben, auf die dieses Richtlinienobjekt angewandt werden soll:
   - Klicken Sie auf **Hinzufügen** und verwenden Sie die Option **Objekte auswählen**, um die gewünschten Objekte auszuwählen.
7. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

- Weitere Informationen über die verfügbaren Richtlinientypen finden Sie unter Bereitstellungsrichtlinienobjekte und Deprovisionsrichtlinienobjekte weiter oben in diesem Dokument.
- Informationen bezüglich der Konfiguration von Richtlinien finden Sie unter Konfigurationsaufgaben für Richtlinien weiter unten in diesem Dokument.
- Um weitere Richtlinien zum neuen Richtlinienobjekt hinzuzufügen, zeigen Sie das Dialogfeld **Eigenschaften** an und klicken Sie dann auf **Hinzufügen** auf der Registerkarte **Richtlinien**.

Hinzufügen, Ändern und Entfernen von Richtlinien

Mit dem Assistenten „Neues Richtlinienobjekt" kann nur eine Richtlinie konfiguriert werden. Ein Richtlinienobjekt kann jedoch mehrere Richtlinien enthalten. Sie können bei einem vorhandenen Richtlinienobjekt Richtlinien hinzufügen, entfernen oder ihre Optionen ändern, indem Sie seine Eigenschaften wie folgt verwalten: Klicken Sie mit der rechten Maustaste auf das Richtlinienobjekt und klicken Sie dann auf **Eigenschaften**.

Um Richtlinien in einem Richtlinienobjekt hinzuzufügen, zu entfernen oder zu bearbeiten, verwenden Sie im Dialogfeld **Eigenschaften** die Registerkarte **Richtlinien**. Die Registerkarte ähnelt der folgenden Abbildung:



Auf der Registerkarte **Richtlinien** wird eine Liste der im Richtlinienobjekt definierten Richtlinien angezeigt. Jeder Listeneintrag enthält ein Symbol, das den Typ der Richtlinie angibt, sowie eine Beschreibung der Richtlinie. Die Richtlinien werden in der Reihenfolge ausgeführt, die in der Liste gezeigt wird. Zum Ändern der Reihenfolge können Sie unten rechts auf der Registerkarte die Reihenfolgeschaltflächen mit den Pfeilen verwenden.

Auf der Registerkarte **Richtlinien** können Sie folgende Verwaltungsaufgaben ausführen:

- **Richtlinie hinzufügen.** Klicken Sie auf die Schaltfläche **Hinzufügen** und folgen Sie den Anweisungen des Assistenten. Diese hängen davon ab, ob Sie ein Richtlinienobjekt für die Bereitstellung oder eines für die Deprovisionierung konfigurieren.

  Der Assistent fordert Sie auf, den Typ der hinzuzufügenden Richtlinie auszuwählen, und führt Sie dann durch die Schritte zum Konfigurieren der Richtlinie. Die Schritte für das Konfigurieren einer Richtlinie hängen vom Richtlinientyp ab. Anweisungen bezüglich der Konfiguration von Richtlinien finden Sie unter „Konfigurationsaufgaben für Richtlinien" weiter unten in diesem Kapitel.

- **Richtlinie löschen.** Wählen Sie in der Liste Richtlinien aus und klicken Sie auf die Schaltfläche **Entfernen**. So werden die ausgewählten Richtlinien permanent gelöscht.

- **Richtlinie ändern.** Wählen Sie eine Richtlinie in der Liste aus und klicken Sie auf die Schaltfläche **Anzeigen/Bearbeiten**. Nun wird das Dialogfeld **Eigenschaften** für die ausgewählte Richtlinie angezeigt.

  Das Dialogfeld **Eigenschaften** enthält mehrere Registerkarten. Jede Registerkarte enthält die gleichen Optionen wie die entsprechende Seite des Assistenten, mit dem die Richtlinie konfiguriert wird. Sie können Richtlinienoptionen hier genauso verwalten wie beim anfänglichen Konfigurationsvorgang.

- **Alle Richtlinien deaktivieren.** Für die Problembehandlung müssen Sie möglicherweise die Durchsetzung der Richtlinien beenden, ohne sie zu löschen. Aktivieren Sie dazu das Kontrollkästchen **Alle in diesem Richtlinienobjekt enthaltenen Richtlinien deaktivieren**.

Welche Richtlinien einem bestimmten Richtlinienobjekt hinzugefügt werden können, hängt vom Typ des Richtlinienobjekts ab. Ein Bereitstellungsrichtlinienobjekt kann nur bereitstellungsrelevante Richtlinien enthalten, während ein Deprovisionsrichtlinienobjekt nur deprovisionsrelevante Richtlinien enthalten kann (siehe „Bereitstellungsrichtlinienobjekte“ und „Richtlinienobjekte zur Bereitstellungsrücknahme“ weiter oben in diesem Kapitel).

Verfahren zum Hinzufügen von Richtlinien zu einem Richtlinienobjekt

Gehen Sie folgendermaßen vor, um eine Richtlinie zu einem Richtlinienobjekt hinzuzufügen:

1. Wählen Sie in der Konsolenstruktur unter **Configuration | Policies | Administration** den Ordner aus, der das Richtlinienobjekt enthält, das Sie ändern möchten.
2. Klicken Sie im Bereich „Details“ mit der rechten Maustaste auf das Richtlinienobjekt und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf der Registerkarte **Richtlinien** auf **Hinzufügen**, um den Assistenten zu starten, der Sie bei der Konfiguration einer Richtlinie unterstützt.
4. Klicken Sie auf der Seite Willkommen des Assistenten auf **Weiter**.
5. Wählen Sie auf der Seite **Zu konfigurierende** Richtlinie den Typ der Richtlinie aus, die Sie dem Richtlinienobjekt hinzufügen möchten.
6. Konfigurieren Sie Richtlinieneinstellungen. Anweisungen finden Sie unter Konfigurationsaufgaben für Richtlinien.

- Auf der Registerkarte **Richtlinien** werden die Richtlinien aufgelistet, die im Richtlinienobjekt konfiguriert sind. Sie können die Registerkarte **Richtlinien** verwenden, um Richtlinien zum Richtlinienobjekt hinzuzufügen, Richtlinien zu ändern oder Richtlinien aus dem Richtlinienobjekt zu löschen.
- Quest One ActiveRoles verarbeitet Richtlinien in der Reihenfolge, in der sie auf der Registerkarte **Richtlinien** aufgeführt sind. Um die Reihenfolge zu ändern, wählen Sie eine Richtlinie aus und klicken Sie dann auf oder , um die Richtlinie nach oben oder unten in der Liste zu verschieben.
- Wenn ein Richtlinienobjekt innerhalb von Quest One ActiveRoles angewandt wird, um Richtlinieneinstellungen im Verzeichnis festzulegen, führen jegliche Änderungen an der Liste der Richtlinien im Richtlinienobjekt dazu, dass die Richtlinieneinstellungen im Verzeichnis entsprechend geändert werden.

Verfahren zum Ändern von Richtlinien in einem Richtlinienobjekt

Gehen Sie folgendermaßen vor, um eine Richtlinie in einem Richtlinienobjekt anzuzeigen oder zu ändern:

1. Wählen Sie in der Konsolenstruktur unter **Configuration | Policies | Administration** den Ordner aus, der das Richtlinienobjekt enthält, das Sie untersuchen möchten.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf das Richtlinienobjekt und klicken Sie dann auf **Eigenschaften**.
3. Wählen Sie auf der Registerkarte **Richtlinien** die anzuzeigende oder zu ändernde Richtlinie aus und klicken Sie auf **Anzeigen/Bearbeiten**.
4. Verwenden Sie die Registerkarten im Dialogfeld **Richtlinieneigenschaften**, um die Richtlinieneinstellungen anzuzeigen oder zu ändern.

   *Die Registerkarten im Dialogfeld **Richtlinieneigenschaften** umfassen die gleichen Optionen wie der Assistent zum Konfigurieren der Richtlinie. Weitere Informationen über die für jeden Richtlinientyp spezifischen Optionen finden Sie unter Konfigurationsaufgaben für Richtlinien.*

- Auf der Registerkarte **Richtlinien** werden die Richtlinien aufgelistet, die im Richtlinienobjekt konfiguriert sind. Sie können die Registerkarte **Richtlinien** verwenden, um Richtlinien zum Richtlinienobjekt hinzuzufügen, Richtlinien zu ändern oder Richtlinien aus dem Richtlinienobjekt zu löschen.
- Quest One ActiveRoles verarbeitet Richtlinien in der Reihenfolge, in der sie auf der Registerkarte **Richtlinien** aufgeführt sind. Um die Reihenfolge zu ändern, wählen Sie eine Richtlinie aus und klicken Sie dann auf oder , um die Richtlinie nach oben oder unten in der Liste zu verschieben.

Verfahren zum Entfernen von Richtlinien aus einem Richtlinienobjekt

Gehen Sie folgendermaßen vor, um eine Richtlinie aus einem Richtlinienobjekt zu löschen:

1. Wählen Sie in der Konsolenstruktur unter **Configuration | Policies | Administration** den Ordner aus, der das Richtlinienobjekt enthält, das Sie ändern möchten.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf das Richtlinienobjekt und klicken Sie dann auf **Eigenschaften**.
3. Wählen Sie auf der Registerkarte **Richtlinien** die Richtlinie aus, die Sie löschen möchten, klicken Sie dann auf **Entfernen** und klicken Sie anschließend auf **Ja**, um den Löschvorgang zu bestätigen.

- Auf der Registerkarte **Richtlinien** werden die Richtlinien aufgelistet, die im Richtlinienobjekt konfiguriert sind. Sie können die Registerkarte **Richtlinien** verwenden, um Richtlinien zum Richtlinienobjekt hinzuzufügen, Richtlinien zu ändern oder Richtlinien aus dem Richtlinienobjekt zu löschen.
- Wenn ein Richtlinienobjekt innerhalb von Quest One ActiveRoles angewandt wird, um Richtlinieneinstellungen im Verzeichnis festzulegen, führen jegliche Änderungen an der Liste der Richtlinien im Richtlinienobjekt dazu, dass die Richtlinieneinstellungen im Verzeichnis entsprechend geändert werden.

Anwenden von Richtlinienobjekten

Das Implementieren einer Richtlinie für die Durchsetzung von Geschäftsregeln umfasst zwei Phasen. Das Konfigurieren der Richtlinie in einem Richtlinienobjekt ist nur der erste Schritt. Beim Erstellen einer neuen Richtlinie wählen Sie aus den verfügbaren Optionen einen Richtlinientyp aus und definieren dann die Optionen, aus denen die Richtlinie besteht. Der zweite Schritt besteht darin, mit Hilfe der Quest One ActiveRoles-Konsole die Richtlinie für die gewünschten Verzeichnisbereiche durchzusetzen.

Mit Quest One ActiveRoles können Richtlinien für ein beliebiges Verzeichnisobjekt durchgesetzt werden, d.h. für eine administrative Ansicht (verwaltete Einheit), einen Verzeichnisordner (Container) oder ein einzelnes Objekt (Blattobjekt). Richtlinien werden durchgesetzt, indem ein Richtlinienobjekt angewendet (verknüpft) wird, das sie enthält.

Wenn Sie ein Richtlinienobjekt auf eine verwaltete Einheit oder einen Verzeichnisordner anwenden, steuern die Richtlinien die Objekte in dieser Einheit oder diesem Ordner sowie auch die Einheit oder den Ordner selbst. Wenn Sie ein Richtlinienobjekt auf ein Blattobjekt anwenden, wie etwa auf einen Benutzer oder eine Gruppe, steuern die Richtlinien nur dieses Objekt. Wenn Sie beispielsweise ein Richtlinienobjekt auf eine Gruppe anwenden, hat dies keine Auswirkungen auf die Mitglieder der Gruppe.

Die Objekte, die einem gegebenen Richtlinienobjekt unterliegen, die also von den in diesem Richtlinienobjekt definierten Richtlinien gesteuert werden, werden als sein *Richtlinienbereich* bezeichnet. Wenn Sie beispielsweise ein Richtlinienobjekt auf eine verwaltete Einheit anwenden, besteht der Richtlinienbereich aus den Objekten innerhalb dieser verwalteten Einheit.

Der Richtlinienbereich enthält also normalerweise alle Objekte in einem Container oder einer verwalteten Einheit, auf den bzw. auf die das Richtlinienobjekt angewendet wird. Manchmal müssen jedoch einzelne Objekte oder Untercontainer aus dem Richtlinienbereich ausgeschlossen werden, damit sich die Richtlinien auf bestimmte Objekte nicht auswirken.

Mit Quest One ActiveRoles können Sie Objekte oder gesamte Container selektiv aus dem Richtlinienbereich ausschließen. Sie können die Vererbung von Richtlinien für einzelne Objekte oder Container blockieren und so den Richtlinienbereich verfeinern. Die Option zum sperren der Richtlinienvererbung wird weiter unten in diesem Abschnitt beschrieben (siehe „Verwalten des Richtlinienbereichs" weiter unten in diesem Kapitel).

Um ein Richtlinienobjekt anzuwenden, können Sie von einem beliebigen der folgenden Punkte aus starten:

- **Richtlinienobjekt.** Fügen Sie dem Richtlinienbereich des Richtlinienobjekts verwaltete Einheiten oder Container hinzu.
- **Verzeichnisobjekt.** Fügen Sie das Richtlinienobjekt der Richtlinienliste für das Verzeichnisobjekt hinzu.

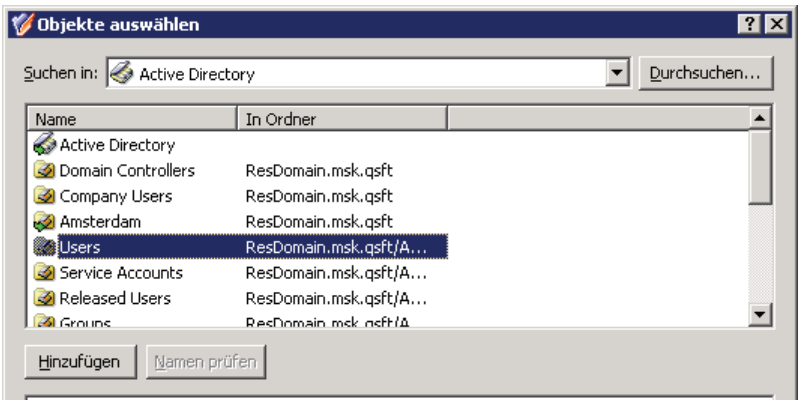
In den folgenden zwei Abschnitten werden diese Optionen ausführlich beschrieben.

Hinzufügen von verwalteten Einheiten oder Containern zu einem Richtlinienbereich

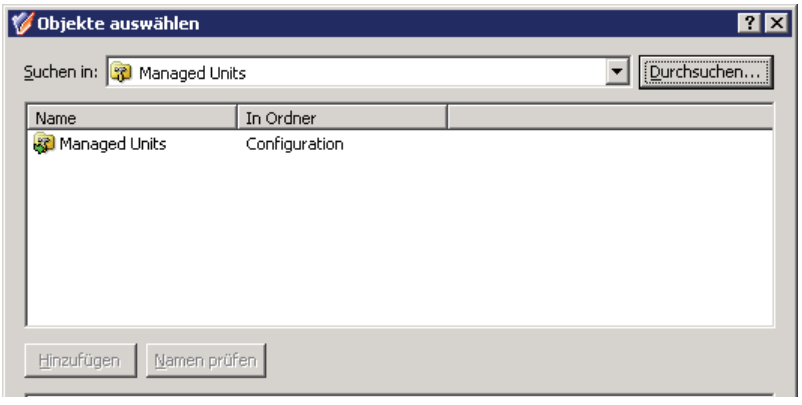
Sie können administrative Ansichten (verwaltete Einheiten) sowie Verzeichnisordner (Container) auf folgende Weisen zum Richtlinienbereich eines bestimmten Richtlinienobjekts hinzufügen:

- Klicken Sie mit der rechten Maustaste auf das Richtlinienobjekt und klicken Sie dann auf **Richtlinienbereich**. Klicken Sie anschließend im Fenster **Quest One ActiveRoles-Richtlinienbereich** auf die Schaltfläche **Hinzufügen**.
- Stellen Sie sicher, dass im Menü **Ansicht** die Option **Erweiterte Detailansicht** aktiviert ist. Wählen Sie dann das Richtlinienobjekt aus. Klicken Sie auf der Registerkarte **Quest One ActiveRoles-Richtlinienbereich** im Detailfenster mit der rechten Maustaste auf einen leeren Bereich und klicken Sie dann auf **Hinzufügen**.

In beiden Fällen wird durch Klicken auf **Hinzufügen** das Fenster **Objekte auswählen** angezeigt, in dem Sie Container und verwaltete Einheiten auswählen können. Um eine Liste auswählbarer Container zu erstellen, klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie **Active Directory** oder einen Container in der Hierarchie unter **Active Directory** aus. Die Liste ähnelt der folgenden Abbildung:



Um eine Liste auswählbarer verwalteter Einheiten zu erstellen, klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie **Verwaltete Einheiten** oder einen Container in der Hierarchie unter **Verwaltete Einheiten** aus. Die Liste ähnelt der folgenden Abbildung:



Wählen Sie im Fenster **Objekte auswählen** in der Liste Container oder verwaltete Einheiten aus und klicken Sie auf die Schaltfläche **Hinzufügen**, um die entstehende Elementliste zu erstellen. Klicken Sie abschließend auf **OK**.

Hinzufügen von Richtlinienobjekten zu Richtlinienlisten für ein Verzeichnisobjekt

Für ein gegebenes Verzeichnisobjekt (Container, Benutzer, Gruppe usw.) wird eine Liste von Richtlinienobjekten, die sich auf das Verzeichnisobjekt auswirken, als *Richtlinienliste* bezeichnet. Wenn das Verzeichnisobjekt sich im Verzeichnisbereich eines gegebenen Richtlinienobjekts befindet, ist das Richtlinienobjekt in die Richtlinienliste dieses Verzeichnisobjekts eingeschlossen.

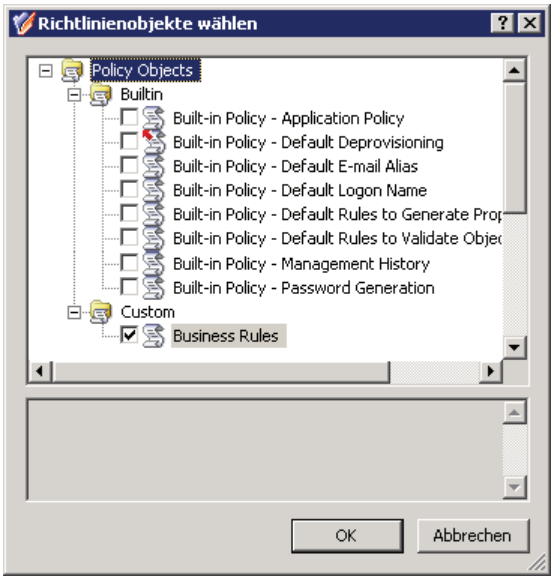
Die Schritte zum Hinzufügen eines Richtlinienobjekts zur Richtlinienliste für ein Verzeichnisobjekt hängen davon ab, ob es ein Container oder ein Blattobjekt ist:

- Klicken Sie mit der rechten Maustaste auf eine verwaltete Einheit oder einen Container und dann auf **Richtlinie erzwingen**. Klicken Sie anschließend im Fenster **Quest One ActiveRoles-Richtlinien** auf die Schaltfläche **Hinzufügen**.
- Klicken Sie mit der rechten Maustaste auf ein Blattobjekt (Benutzer, Gruppe o.ä.) und dann auf **Eigenschaften**, öffnen Sie die Registerkarte **Verwaltung** und klicken Sie auf die Schaltfläche **Richtlinie**. Klicken Sie anschließend im Fenster **Quest One ActiveRoles-Richtlinien** auf die Schaltfläche **Hinzufügen**.

Wenn Sie den erweiterten Bereich „Details" verwenden (d.h. wenn im Menü **Ansicht** die Option **Erweiterte Detailansicht** aktiviert ist), können Sie dies unabhängig vom Typ des Verzeichnisobjekts wie folgt erreichen:

- Wählen Sie das Verzeichnisobjekt aus, öffnen Sie im Bereich „Details" die Registerkarte **ActiveRoles-Richtlinie**, klicken Sie mit der rechten Maustaste in einen leeren Bereich auf der Registerkarte und klicken Sie dann auf **Hinzufügen**.

In allen Fällen wird durch Klicken auf **Hinzufügen** das Fenster **Richtlinienobjekte wählen** angezeigt, in dem Sie hinzuzufügende Richtlinienobjekte auswählen können. Aktivieren Sie die Kontrollkästchen neben den Namen von Richtlinienobjekten, wie in der folgenden Abbildung gezeigt, und klicken Sie dann auf **OK**.



Verfahren zum Anwenden eines Richtlinienobjekts

So wenden Sie ein Richtlinienobjekt an:

1. Wählen Sie in der Konsolenstruktur unter **Configuration | Policies | Administration** den Ordner aus, der das Richtlinienobjekt enthält, das Sie anwenden möchten.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf das Richtlinienobjekt und klicken Sie dann auf **Richtlinienbereich**.
3. Klicken Sie im Dialogfeld **Quest One ActiveRoles-Richtlinienbereich** auf **Hinzufügen**.
4. Verwenden Sie das Dialogfeld **Objekte auswählen**, um den Container, die verwaltete Einheit oder das Objekt auszuwählen, für das Sie Richtlinieneinstellungen mit Hilfe des Richtlinienobjekts festlegen möchten.
5. Klicken Sie auf **OK**, um das Dialogfeld **Quest One ActiveRoles-Richtlinienbereich** zu schließen.

Gehen Sie folgendermaßen vor, um die Richtlinieneinstellungen für ein Objekt mit Hilfe eines Richtlinienobjekts anzugeben:

1. Zeigen Sie das Dialogfeld **Quest One ActiveRoles-Richtlinie** für das Objekt an:
   - Klicken Sie mit der rechten Maustaste auf das Objekt und klicken Sie dann auf **Richtlinie erzwingen**.

   – ODER –

   - Klicken Sie mit der rechten Maustaste auf das Objekt und klicken Sie dann auf **Eigenschaften**. Klicken Sie dann auf der Registerkarte **Verwaltung** im Dialogfeld **Eigenschaften** auf **Richtlinie**.
2. Klicken Sie in dem Dialogfeld **Quest One ActiveRoles Richtlinien** auf **Hinzufügen**.
3. Verwenden Sie das Dialogfeld **Richtlinienobjekte wählen**, um das anzuwendende Richtlinienobjekt auszuwählen.

   Um ein Richtlinienobjekt auszuwählen, aktivieren Sie das Kontrollkästchen neben dem Namen des Richtlinienobjekts. Sie können mehrere Richtlinienobjekte auswählen.
4. Klicken Sie auf **OK**, um das Dialogfeld **Quest One ActiveRoles-Richtlinie** zu schließen.

Um ein Richtlinienobjekt anzuwenden, können Sie auch die Registerkarte **Quest One ActiveRoles-Richtlinienbereich** oder **ActiveRoles-Richtlinie** in der erweiterten Detailanzeige verwenden: Klicken Sie mit der rechten Maustaste auf einen freien Bereich auf der Registerkarte und klicken Sie dann auf **Hinzufügen**. Um die erweiterte Detailanzeige anzuzeigen, aktivieren Sie **Erweiterte Detailansicht** im Menü **Ansicht** (siehe Erweiterter Bereich weiter oben in diesem Dokument).

Gehen Sie folgendermaßen vor, um Vererbungsoptionen für ein Richtlinienobjekt für einen Container oder eine verwaltete Einheit anzuzeigen oder zu ändern:

1. Zeigen Sie das Dialogfeld **Quest One ActiveRoles-Richtlinienbereich** für das Richtlinienobjekt an: Klicken Sie mit der rechten Maustaste auf das Richtlinienobjekt und klicken Sie dann auf **Richtlinienbereich**.
2. Wählen Sie im Dialogfeld **Quest One ActiveRoles-Richtlinienbereich** den Container oder die verwaltete Einheit aus, auf das das Richtlinienobjekt angewandt wird und dessen Vererbungsoptionen Sie überprüfen möchten, und klicken Sie dann auf **Anzeigen/ Bearbeiten**.
3. Zeigen Sie auf der Registerkarte **Allgemein** die Auswahl dieser Optionen, die den Bereich festlegt, in dem das Richtlinienobjekt die Richtlinieneinstellungen festlegt, an und ändern Sie diese:
   - **Dieses Verzeichnisobjekt.** Der Bereich umfasst den Container oder die verwaltete Einheit, den bzw. die Sie ausgewählt haben (diese Option führt nicht dazu, dass der Bereich die untergeordneten Objekte oder Mitglieder des Containers oder der verwalteten Einheit enthält).

- **Untergeordnete Objekte dieses Verzeichnisobjekts.** Der Bereich umfasst alle untergeordneten Objekte (oder Mitglieder bei Anwendung auf eine verwaltete Einheit) in der gesamten Hierarchie unter dem von Ihnen ausgewählten Container oder unter der von Ihnen ausgewählten verwalteten Einheit.
- **Nur unmittelbar untergeordnete Objekte.** Der Bereich umfasst nur die untergeordneten Objekte (oder Mitglieder bei einer verwalteten Einheit), denen der von Ihnen ausgewählte Container oder die von Ihnen ausgewählte verwaltete Einheit direkt übergeordnet ist.

Verwalten des Richtlinienbereichs

Beim Anwenden eines Richtlinienobjekts auf ein Verzeichnisobjekt erstellt Quest One ActiveRoles eine Richtlinienobjektverknüpfung. Richtlinien werden also durch Verknüpfen von Richtlinienobjekten mit Verzeichnisobjekten aktiviert, d.h. mit verwalteten Einheiten, Verzeichnisordnern (Containern) oder einzelnen Objekten (Blattobjekten).

Jede Richtlinienobjektverknüpfung enthält die folgenden Informationen:

- Das Richtlinienobjekt, das die Richtlinien definiert
- Das Verzeichnisobjekt, das Ziel der Verknüpfung ist
- Das Flag (**Einschließen** oder **Ausschließen**), das angibt, ob das Verzeichnisobjekt in den Richtlinienbereich eingeschlossen wird

Sie können über eine der folgenden Möglichkeiten eine Liste von Richtlinienobjekten anzeigen:

- **Richtlinienobjekt.** Klicken Sie mit der rechten Maustaste auf ein Richtlinienobjekt und klicken Sie dann auf **Richtlinienbereich**.

  Dies zeigt die Verknüpfungen an, in denen das Richtlinienobjekt auftritt.

- **Verzeichnisobjekt.** Öffnen Sie zunächst wie folgt ein Fenster mit einer Liste der Richtlinienobjekte, die sich auf dieses Verzeichnisobjekt auswirken:

  - Auf ein Containerobjekt oder eine verwaltete Einheit klicken Sie mit der rechten Maustaste und klicken Sie dann auf **Richtlinie erzwingen**.
  - Für ein Blattobjekt öffnen Sie das Dialogfeld **Eigenschaften** öffnen die Registerkarte **Verwaltung** und klicken auf **Richtlinie**.

  Im nun geöffneten Fenster klicken Sie auf die Schaltfläche **Erweitert**.

  Damit werden die Verknüpfungen angezeigt, in denen das Verzeichnisobjekt als Zielobjekt auftritt.

Sie können eine Liste von Richtlinienobjektverknüpfungen auch über den erweiterten Bereich „Details" anzeigen. Stellen Sie sicher, dass im Menü **Ansicht** die Option **Erweiterte Detailansicht** aktiviert ist, und führen Sie dann eine der folgenden Aktionen aus:

- Wählen Sie ein Richtlinienobjekt aus.

  Auf der Registerkarte **Quest One ActiveRoles-Richtlinienbereich** werden die Verknüpfungen aufgelistet, in denen das ausgewählte Richtlinienobjekt auftritt.

- Wählen Sie ein Verzeichnisobjekt (verwaltete Einheit, Container oder Blattobjekt) aus, klicken Sie mit der rechten Maustaste in einen leeren Bereich auf der Registerkarte **ActiveRoles-Richtlinie** und klicken Sie dann auf **Erweiterte Ansicht**.

  Damit werden die Verknüpfungen angezeigt, in denen das Verzeichnisobjekt als Zielobjekt auftritt.

Wenn Sie eine Liste von Richtlinienobjektverknüpfungen für ein Verzeichnisobjekt anzeigen, wird die Liste in einem separaten Fenster angezeigt. Jeder Eintrag in der Liste schließt die folgenden Informationen ein:

- **Richtlinienobjekt.** Name des Richtlinienobjekts.
- **Verzeichnisobjekt.** Kanonischer Name des Objekts, mit dem das Richtlinienobjekt verknüpft ist, d.h. des Zielobjekts der Verknüpfung.
- **Einschließen/Ausschließen**- Flag, der das Verhalten der Verknüpfung angibt:
  - **Explizit einschließen** bedeutet, dass die Verknüpfung das Zielobjekt in den Richtlinienbereich aufnimmt, d.h. dass die im Richtlinienobjekt definierten Richtlinien das Zielobjekt steuern.
  - **Explizit ausschließen** bedeutet, dass die Verknüpfung das Zielobjekt nicht in den Richtlinienbereich aufnimmt, d.h. dass die im Richtlinienobjekt definierten Richtlinien das Zielobjekt nicht steuern.

Das Flag **Ausschließen** hat Vorrang vor dem Flag **Einschließen** Wenn zwei Verknüpfungen mit demselben Richtlinienobjekt vorhanden sind, von denen eine das Flag **Einschließen** und die andere das Flag **Ausschließen** aufweist, wird das Objekt aus dem Richtlinienbereich des Richtlinienobjekts ausgeschlossen.

In der Liste der Richtlinienobjektverknüpfungen werden die Verknüpfungen der folgenden Kategorien angezeigt:

- **Direkte Verknüpfungen.** Das Richtlinienobjekt wird direkt auf das ausgewählte Objekt angewendet (mit ihm verknüpft).
- **Geerbte Verknüpfungen.** Das Richtlinienobjekt wird auf einen Container in der Containerhierarchie über dem ausgewählten Objekt oder auf eine verwaltete Einheit, zu der das ausgewählte Objekt gehört, angewendet (mit ihm/ihr verknüpft).

Die von übergeordneten Objekte geerbten Verknüpfungen können aus der Liste herausgefiltert werden. Deaktivieren Sie hierzu das Kontrollkästchen **Vererbung anzeigen**.

Zum Verwalten von Verknüpfungen können Sie die Schaltflächen unter der Liste verwenden:

- **Hinzufügen.** Zeigt das Dialogfeld an, in dem Sie Richtlinienobjekte auswählen können, um Verknüpfungen zu ihnen zu erstellen.
- **Entfernen.** Löscht die ausgewählten Einträge aus der Verknüpfungsliste. Nur für direkte Verknüpfungen verfügbar.
- **Anzeigen/Bearbeiten.** Zeigt das Dialogfeld zum Anzeigen oder Ändern von Verknüpfungseigenschaften an (z.B. der Eigenschaft), die angibt, ob die Verknüpfung sich auf die untergeordneten Objekten ihres Zielobjekts auswirkt. Nur für die Verknüpfungen mit dem Flag **Einschließen** verfügbar.
- **Ausschließen.** Wird für Verknüpfungen angezeigt, die mit dem Flag **Einschließen** gekennzeichnet sind. Nur für direkte Verknüpfungen verfügbar. Ändert den Flag in **Ausschließen**.
- **Einschließen.** Wird für Verknüpfungen angezeigt, die mit dem Flag **Ausschließen** gekennzeichnet sind. Nur für direkte Verknüpfungen verfügbar. Ändert den Flag auf **Einschließen**.

Die Schaltfläche **Entfernen** ist nur für direkte Verknüpfungen verfügbar. Wenn Sie Verknüpfungen löschen möchten, sollten Sie sie mit dem Befehl **Richtlinienbereich** für das Richtlinienobjekt verwalten.

Um die Verwaltung der Auswirkungen von Richtlinien auf Verzeichnisobjekte zu vereinfachen, ermöglicht Ihnen die Quest One ActiveRoles-Konsole das Verwalten des Richtlinienbereichs ohne direktes Verwalten von Verknüpfungen mit Richtlinienobjekten. Die Richtlinienliste eines Verzeichnisobjekts ist eine Liste der Richtlinienobjekte, die das Verzeichnisobjekt steuern, d.h. sich auf es auswirken. Sie können diese Richtlinienliste anzeigen und ändern, statt durch direkte und indirekte Verknüpfungen navigieren zu müssen.

Sie können die Richtlinienliste eines gegebenen Verzeichnisobjekts wie folgt anzeigen:

- Auf einen Container oder eine verwaltete Einheit klicken Sie mit der rechten Maustaste und klicken dann auf **Richtlinie erzwingen**
- Auf ein Blattobjekt (Benutzer, Gruppe o.ä.) klicken Sie mit der rechten Maustaste, klicken Sie dann auf **Eigenschaften**, öffnen Sie die Registerkarte **Verwaltung** und klicken Sie auf die Schaltfläche **Richtlinie**.

Jeder Eintrag in der Richtlinienliste schließt die folgenden Informationen ein:

- **Richtlinienobjekt.** Der Name des Richtlinienobjekts. Das Richtlinienobjekt steuert dieses Verzeichnisobjekt aufgrund einer direkten Verknüpfung oder geerbter Verknüpfungen.
- **Vererbung blockieren.** Zeigt an, ob die Auswirkung der Richtlinie für dieses Verzeichnisobjekt blockiert ist. Wenn das Kontrollkästchen **Gesperrt** aktiviert ist, wird die Richtlinienobjektverknüpfung mit dem Flag **Ausschließen** für dieses Verzeichnisobjekt erstellt.

Sie können die Richtlinienliste mit Hilfe der Schaltflächen unter der Liste verwalten:

- **Hinzufügen.** Zeigt das Dialogfeld an, in dem Sie Richtlinienobjekte auswählen können, um das Verzeichnisobjekt ihrer Steuerung zu unterstellen.
- **Entfernen.** Wenn Sie in der Richtlinienliste ein Richtlinienobjekt auswählen und auf **Entfernen** klicken, wird die direkte Verknüpfung des Richtlinienobjekts mit diesem Objekt gelöscht.

  Wenn sich das Richtlinienobjekt aufgrund einer geerbten Verknüpfung in der Liste befindet, ist die Schaltfläche **Entfernen** nicht verfügbar. Wenn außerdem sowohl die direkte Verknüpfung als auch eine geerbte Verknüpfung für das Richtlinienobjekt vorhanden sind, wird durch Klicken auf **Entfernen** die direkte Verknüpfung gelöscht, aber *nicht* das Richtlinienobjekt aus der Richtlinienliste gelöscht. In diesem Fall verbleibt das Richtlinienobjekt in der Liste, weil die Richtlinien aufgrund der Vererbung weiterhin angewendet werden.

  Wenn Sie das Verzeichnisobjekt aus dem Richtlinienbereich eines bestimmten Richtlinienobjekts entfernen möchten, aktivieren Sie das Kontrollkästchen **Gesperrt** in der Spalte **Vererbung blockieren**. Dies fügt die Richtlinienobjektverknüpfung mit dem Flag **Ausschließen** für das Verzeichnisobjekt hinzu.
- **Anzeigen/Bearbeiten.** Zeigt das Dialogfeld **Eigenschaften** für das Richtlinienobjekt an, das Sie in der Liste auswählen. Mit dem Dialogfeld **Eigenschaften** können Sie Richtlinien im Richtlinienobjekt verwalten und Zugriff auf die Liste aller Verknüpfungen erhalten, in denen dieses Richtlinienobjekt vorkommt.
- **Erweitert.** Öffnet das Fenster mit der Liste der Richtlinienobjektverknüpfungen für dieses Verzeichnisobjekt, die weiter oben in diesem Abschnitt erörtert wird.

Sie können auf die Richtlinienliste auch über den erweiterten Bereich „Details" zugreifen. Die Liste wird auf der Registerkarte **ActiveRoles-Richtlinie** angezeigt, wenn Sie ein Verzeichnisobjekt auswählen.

Auf der Registerkarte **ActiveRoles-Richtlinie** können Sie die die gleichen Verwaltungsaufgaben ausführen wie im Fenster **Quest One ActiveRoles-Richtlinie**: Klicken Sie mit der rechten Maustaste auf einen Listeneintrag oder in einen leeren Bereich, und verwenden Sie Befehle aus dem Kontextmenü. Die Befehle haben die gleichen Funktionen wie die Schaltflächen im Fenster **Quest One ActiveRoles-Richtlinie**.

Sie können den Richtlinienbereich eines gegebenen Richtlinienobjekts auch mit Hilfe einer Liste von Verzeichnisobjekten verwalten, auf die das Richtlinienobjekt angewendet wird (mit denen es verknüpft ist). Die Liste kann in einem separaten Fenster oder auf einer Registerkarte im erweiterten Bereich „Details" angezeigt werden:

- Um die Liste in einem Fenster anzuzeigen, klicken Sie mit der rechten Maustaste auf das Richtlinienobjekt und klicken dann auf **Richtlinienbereich**.
- Um die Liste auf einer Registerkarte anzuzeigen, stellen Sie sicher, dass im Menü **Ansicht** die Option **Erweiterte Detailansicht** aktiviert ist, und wählen Sie das Richtlinienobjekt aus.

In der Liste werden alle Verknüpfungen des Richtlinienobjekts angezeigt. Jeder Eintrag in der Liste schließt die folgenden Informationen ein:

- **Name.** Kanonischer Name des Verzeichnisobjekts, mit dem das Richtlinienobjekt verknüpft ist, d.h. des Zielobjekts der Verknüpfung.
- **Einschließen/Ausschließen.** Flag, der das Verhalten der Verknüpfung angibt:
  - **Explizit einschließen** bedeutet, dass die Verknüpfung das Zielobjekt in den Richtlinienbereich aufnimmt, d.h. dass die im Richtlinienobjekt definierten Richtlinien das Zielobjekt steuern.
  - **Explizit ausschließen** bedeutet, dass die Verknüpfung das Zielobjekt nicht in den Richtlinienbereich aufnimmt, d.h. dass die im Richtlinienobjekt definierten Richtlinien das Zielobjekt nicht steuern.

  Das Flag **Ausschließen** hat Vorrang vor dem Flag **Einschließen** Wenn zwei Verknüpfungen mit demselben Zielobjekt vorhanden sind, von denen eine das Flag **Einschließen** und die andere das Flag **Ausschließen** aufweist, wird das Zielobjekt aus dem Richtlinienbereich des Richtlinienobjekts ausgeschlossen.

Zum Verwalten der Liste im Fenster **Quest One ActiveRoles-Richtlinienbereich** können Sie die Schaltflächen unterhalb der Liste verwenden: **Hinzufügen**, **Entfernen**, **Anzeigen/Bearbeiten** und **Einschließen** oder **Ausschließen**. Diese Schaltflächen haben etwa die gleichen Funktionen wie die weiter oben in diesem Abschnitt bei der Erörterung der Verwaltungsaufgaben für Richtlinienobjektverknüpfungen beschriebenen. Zum Verwalten der Liste auf der Registerkarte **Quest One ActiveRoles-Richtlinienbereich** können Sie die Befehle im Kontextmenü verwenden: Klicken Sie mit der rechten Maustaste auf eine Verknüpfung oder in einen leeren Bereich, um auf das Menü zuzugreifen. Das Menü enthält die folgenden Befehle:

- **Hinzufügen.** Wird angezeigt, wenn Sie mit der rechten Maustaste in einen leeren Bereich klicken. Führt die gleiche Aktion aus wie die Schaltfläche **Hinzufügen**. Öffnet das Dialogfeld **Objekte auswählen**, in dem Sie Container oder verwaltete Einheiten auswählen können, mit denen Sie das Richtlinienobjekt verknüpfen möchten (siehe auch Anwenden von Richtlinienobjekten).
- **Löschen.** Wird angezeigt, wenn Sie mit der rechten Maustaste auf eine Verknüpfung klicken. Führt die gleiche Aktion aus wie die Schaltfläche **Entfernen**. Löscht die ausgewählte Verknüpfung aus der Liste.

- **Ausschließen.** Wird angezeigt, wenn Sie mit der rechten Maustaste auf eine Verknüpfung mit dem Flag **Einschließen** klicken. Führt die gleiche Aktion aus wie die Schaltfläche **Ausschließen**. Ändert das Flag für die ausgewählte Verknüpfung.
- **Einschließen.** Wird angezeigt, wenn Sie mit der rechten Maustaste auf eine Verknüpfung mit dem Flag **Ausschließen** klicken. Führt die gleiche Aktion aus wie die Schaltfläche **Einschließen**. Ändert das Flag für die ausgewählte Verknüpfung.
- **Aktualisieren.** Aktualisiert die Liste mit den aktuellen Informationen.

Verfahren zum Verwalten von Richtlinienobjektverknüpfungen

Wenn Sie ein Richtlinienobjekt anwenden (siehe Anwenden von Richtlinienobjekten weiter oben in diesem Dokument), erstellt Quest One ActiveRoles ein Objekt, das als eine *Richtlinienobjektverknüpfung* bezeichnet wird und das Informationen über das Richtlinienobjekt und das Verzeichnisobjekt speichert, auf die das Richtlinienobjekt angewandt wird. Im Großen und Ganzen entspricht die Verwaltung von Richtlinieneinstellungen in Quest One ActiveRoles der Verwaltung von Richtlinienobjekten und Richtlinienobjektverknüpfungen. In diesem Thema sind einige Anleitungen aufgeführt, die Sie zum Anzeigen und Ändern von Richtlinienobjektverknüpfungen verwenden können.

Gehen Sie folgendermaßen vor, um Richtlinienobjektverknüpfungen anzuzeigen oder zu ändern, in denen ein bestimmtes Richtlinienobjekt vorkommt:

1. Klicken Sie mit der rechten Maustaste auf das Richtlinienobjekt und klicken Sie dann auf **Richtlinienbereich**.
2. Nehmen Sie im Dialogfeld **Quest One ActiveRoles-Richtlinienbereich** Folgendes vor:
   - Um eine neue Verknüpfung zu erstellen, klicken Sie auf **Hinzufügen** und verwenden Sie dann das Dialogfeld Objekte auswählen, um das **Objekt auszuwählen**, mit dem Sie das Richtlinienobjekt verknüpfen möchten.
   - Um eine Verknüpfung zu löschen, wählen Sie sie aus der Liste aus und klicken Sie dann auf **Entfernen**.
   - Um die Eigenschaften einer Verknüpfung wie etwa die Vererbungsoptionen anzuzeigen oder zu ändern, wählen Sie die Verknüpfung aus der Liste aus und klicken Sie dann auf **Anzeigen/Bearbeiten**. Weitere Informationen über Vererbungsoptionen finden Sie unter Verfahren zum Anwenden eines Richtlinienobjekts weiter oben in diesem Dokument.)
   - Um anzugeben, ob eine Verknüpfung die Auswirkungen des Richtlinienobjekts auf das Objekt, mit dem das Richtlinienobjekt verknüpft ist, aufhebt oder anwendet, wählen Sie die Verknüpfung aus und klicken Sie dann auf **Ausschließen** bzw. **Einschließen**.

Gehen Sie folgendermaßen vor, um eine Liste der Richtlinienobjekte anzuzeigen oder zu ändern, die die Richtlinieneinstellungen für ein bestimmtes Objekt bestimmen:

1. Zeigen Sie das Dialogfeld **Quest One ActiveRoles-Richtlinie** für das Objekt an:
   - Klicken Sie mit der rechten Maustaste auf das Objekt und klicken Sie dann auf **Richtlinie erzwingen**.

   – ODER –

   - Klicken Sie mit der rechten Maustaste auf das Objekt und klicken Sie dann auf **Eigenschaften**. Klicken Sie dann auf der Registerkarte **Verwaltung** im Dialogfeld **Eigenschaften** auf **Richtlinie**.

   *Das Dialogfeld **Quest One ActiveRoles-Richtlinie** für ein bestimmtes Objekt listet alle Richtlinienobjekte auf, die die Richtlinieneinstellungen für dieses Objekt bestimmen. Gehen Sie wie nachfolgend beschrieben vor, um die Liste bei Bedarf zu ändern.*

2. Nehmen Sie im Dialogfeld **Quest One ActiveRoles-Richtlinie** Folgendes vor:
   - Um weitere Richtlinieneinstellungen für das Objekt zu definieren, klicken Sie auf **Hinzufügen** und wählen Sie dann ein oder mehrere Richtlinienobjekte aus, die die Richtlinieneinstellungen festlegen.
   - Um die Auswirkung eines bestimmten Richtlinienobjekts auf das von Ihnen verwaltete Objekt zu unterbinden, aktivieren Sie das Kontrollkästchen **Gesperrt** neben dem Namen des Richtlinienobjekts. Deaktivieren Sie das Kontrollkästchen, wenn Sie möchten, dass das Richtlinienobjekt Auswirkungen auf das Objekt haben soll.
   - Um eine Richtlinienobjektverknüpfung für das Objekt zu löschen, wählen Sie das Richtlinienobjekt aus und klicken Sie dann auf **Entfernen**. (Dieser Vorgang kann durchgeführt werden, wenn das Richtlinienobjekt mit dem Objekt selbst und nicht mit einem Container oder einer verwalteten Einheit, in der sich das Objekt befindet, verknüpft ist.)
   - Um Richtlinien in einem Richtlinienobjekt anzuzeigen oder zu ändern, wählen Sie das Richtlinienobjekt aus und klicken Sie dann auf **Anzeigen/Bearbeiten**. (Weitere Anweisungen finden Sie unter Verfahren zum Ändern von Richtlinien in einem Richtlinienobjekt weiter oben in diesem Dokument.)
   - Um eine Liste der Richtlinienobjektverknüpfungen anzuzeigen, die die Richtlinieneinstellungen für das Objekt festlegen, klicken Sie auf **Erweitert**. Gehen Sie wie nachfolgend beschrieben vor, um die Liste bei Bedarf zu verwalten.

Gehen Sie folgendermaßen vor, um Richtlinienobjektverknüpfungen anzuzeigen oder zu ändern, die die Richtlinieneinstellungen für ein bestimmtes Objekt bestimmen:

1. Klicken Sie im Dialogfeld **Quest One ActiveRoles-Richtlinie** auf **Erweitert**.
2. Nehmen Sie im Dialogfeld **Quest One ActiveRoles-Richtlinie - Erweiterte Ansicht** Folgendes vor:
   - Um eine neue Verknüpfung zu erstellen, klicken Sie auf **Hinzufügen** und wählen Sie dann das gewünschte Richtlinienobjekt aus.
   - Um eine Verknüpfung zu löschen, wählen Sie sie aus der Liste aus und klicken Sie dann auf **Entfernen**. (Dieser Vorgang kann durchgeführt werden, wenn das Richtlinienobjekt mit dem Objekt selbst und nicht mit einem Container oder einer verwalteten Einheit, in der sich das Objekt befindet, verknüpft ist.)
   - Um die Eigenschaften einer Verknüpfung wie etwa die Vererbungsoptionen anzuzeigen oder zu ändern, wählen Sie die Verknüpfung aus der Liste aus und klicken Sie dann auf **Anzeigen/Bearbeiten**.
   - Um anzugeben, ob eine Verknüpfung die Auswirkungen des Richtlinienobjekts auf das von Ihnen verwaltete Objekt aufhebt oder anwendet, wählen Sie die Verknüpfung aus und klicken Sie dann auf **Ausschließen** bzw. **Einschließen**.

- Standardmäßig führt das Dialogfeld **Quest One ActiveRoles-Richtlinie – Erweiterte Ansicht** für ein Objekt alle Verknüpfungen auf, die die Richtlinieneinstellungen für das Objekt festlegen, und zwar unabhängig davon, ob eine Verknüpfung für das Objekt selbst oder für einen Container oder eine verwaltete Einheit, in der sich das Objekt befindet, erstellt wurde. Um die Anzeige der Liste zu ändern, deaktivieren Sie das Kontrollkästchen **Vererbung anzeigen**.
- Im Dialogfeld **Quest One ActiveRoles-Richtlinie – Erweiterte Ansicht** können nur direkte Verknüpfungen entfernt werden. Das heißt, dass eine Verknüpfung entfernt werden kann, wenn die Verknüpfung für das Objekt selbst erstellt wurde (und nicht von einem Container oder einer verwaltete Einheit geerbt wurde). Wenn Sie das Kontrollkästchen **Vererbung anzeigen** deaktivieren, werden nur direkte Verknüpfungen angezeigt. Sie können sie löschen, indem Sie auf **Entfernen** klicken.

- Durch Anklicken von **Anzeigen/Bearbeiten** im Dialogfeld **Quest One ActiveRoles-Richtlinie – Erweiterte Ansicht** oder **Quest One ActiveRoles-Richtlinienbereich** wird das Dialogfeld **Eigenschaften** für die ausgewählte Verknüpfung angezeigt. Ausgehend vom Dialogfeld **Eigenschaften** können Sie auf die Eigenschaften sowohl des von der Verknüpfung abgedeckten Verzeichnisobjekts als auch des ebenfalls von der Verknüpfung abgedeckten Richtlinienobjekts zugreifen und die Vererbungsoptionen für die Verknüpfungen anzeigen und ändern (siehe Verfahren zum Anwenden eines Richtlinienobjekts weiter oben in diesem Dokument).
- Sie können auch die Richtlinienobjektverknüpfungen auf der Registerkarte **Quest One ActiveRoles-Richtlinienbereich** oder **ActiveRoles-Richtlinie** in der erweiterten Detailanzeige verwalten, die es Ihnen ermöglicht, dieselben Aufgaben wie im Dialogfeld **Quest One ActiveRoles-Richtlinienbereich** bzw. **Quest One ActiveRoles-Richtlinie** durchzuführen. Klicken Sie mit der rechten Maustaste auf eine Verknüpfung oder in einen leeren Bereich auf der Registerkarte und verwenden Sie Befehle aus dem Kontextmenü. Die Registerkarte **Quest One ActiveRoles-Richtlinienbereich** wird angezeigt, wenn Sie ein Richtlinienobjekt auswählen. Andernfalls wird die Registerkarte **ActiveRoles-Richtlinie** angezeigt. Um die erweiterte Detailanzeige anzuzeigen, aktivieren Sie **Erweiterte Detailansicht** im Menü **Ansicht** (siehe Erweiterter Bereich weiter oben in diesem Dokument).

Verfahren zum Ausschließen eines Objekts aus einem Richtlinienbereich

Die Objekte, auf die ein bestimmtes Richtlinienobjekt Einfluss hat, werden gemeinhin als der Richtlinienbereich des Richtlinienobjekts bezeichnet. Wenn Sie ein Richtlinienobjekt anwenden, fügen Sie Objekte zum Richtlinienbereich hinzu. Gehen Sie wie nachfolgend beschrieben vor, um bestimmte Objekte aus dem Richtlinienbereich eines Richtlinienobjekts auszuschließen, um die Auswirkungen des Richtlinienobjekts auf diese Objekte zu vermeiden.

Gehen Sie folgendermaßen vor, um ein Objekt aus dem Richtlinienbereich eines Richtlinienobjekts auszuschließen:

1. Zeigen Sie das Dialogfeld **Quest One ActiveRoles-Richtlinie** für das Objekt an:
   - Klicken Sie mit der rechten Maustaste auf das Objekt und klicken Sie dann auf **Richtlinie erzwingen**.

   – ODER –

   - Klicken Sie mit der rechten Maustaste auf das Objekt und klicken Sie dann auf **Eigenschaften**. Klicken Sie dann auf der Registerkarte **Verwaltung** im Dialogfeld **Eigenschaften** auf **Richtlinie**.
2. Aktivieren Sie im Dialogfeld **Quest One ActiveRoles-Richtlinie** das Kontrollkästchen **Gesperrt** neben dem Namen des Richtlinienobjekts.
3. Klicken Sie auf **OK**, um das Dialogfeld **Quest One ActiveRoles-Richtlinie** zu schließen.

- Sie können die Auswirkungen des Richtlinienobjekts auf das Objekt, das aus dem Richtlinienbereich ausgeschlossen wurde, wiederherstellen: Deaktivieren Sie im Dialogfeld **Quest One ActiveRoles-Richtlinie** für das Objekt das Kontrollkästchen **Gesperrt** neben dem Namen des Richtlinienobjekts.
- Durch das Ausschließen eines Objekts aus dem Richtlinienbereich wird eine Richtlinienobjektverknüpfung für dieses Objekt erstellt, wobei die Verknüpfung als „Explizit ausschließen" gekennzeichnet wird. Die Wiederherstellung der Auswirkungen des Richtlinienobjekts führen zum Entfernen dieser Verknüpfung. Anweisungen bezüglich der Verwaltung von Richtlinienobjektverknüpfungen Sie unter Verfahren zum Verwalten von Richtlinienobjektverknüpfungen weiter oben in diesem Dokument.

Kopieren eines Richtlinienobjekts

Mit der Quest One ActiveRoles-Konsole können Sie Kopien von Richtlinienobjekten erstellen. Mit dieser Funktion können Sie vorhandene Richtlinienobjekte wieder verwenden.

Zum Erstellen einer Kopie eines Richtlinienobjekts klicken Sie mit der rechten Maustaste auf das Richtlinienobjekt und klicken Sie dann auf **Kopieren**. Hierdurch wird der Assistent „Objekt kopieren" geöffnet. Geben Sie einen Namen und eine Beschreibung für die Kopie ein und klicken Sie dann auf **Weiter**.

Auf der nächsten Seite des Assistenten wird eine Liste von Richtlinien angezeigt. Die Liste enthält alle im ursprünglichen Richtlinienobjekt definierten Richtlinien. Klicken Sie auf **Fertig stellen**, um die Kopie zu erstellen.

Die Kopie besitzt die gleichen Eigenschaften wie das ursprüngliche Richtlinienobjekt, einschließlich der Richtlinien und ihrer Konfigurationen. Sie können im Dialogfeld **Eigenschaften** Änderungen an der Kopie wie weiter oben in diesem Kapitel beschrieben vornehmen (siehe Hinzufügen, Ändern und Entfernen von Richtlinien).

Verfahren zum Kopieren eines Richtlinienobjekts

So kopieren Sie ein Richtlinienobjekt:

1. Wählen Sie in der Konsolenstruktur unter **Configuration | Policies | Administration** den Ordner aus, der das Richtlinienobjekt enthält, das Sie kopieren möchten.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf das Richtlinienobjekt und klicken Sie dann auf **Kopieren**, um den Assistenten „Objekt kopieren – Richtlinienobjekt" zu starten.
3. Gehen Sie auf der ersten Seite des Assistenten wie folgt vor und klicken Sie dann auf **Weiter**:
   a) Geben Sie in das Feld **Name** den Namen des neuen Richtlinienobjekts ein.
   b) Geben Sie im Feld **Beschreibung** optionale Informationen über das neue Richtlinienobjekt ein.
4. Klicken Sie auf **Fertig stellen**, um die Erstellung des neuen Richtlinienobjekts abzuschließen.

Die Kopie eines Richtlinienobjekts enthält dieselben Richtlinien wie das Original-Richtlinienobjekt. Sie können Richtlinien mit Hilfe des Dialogfelds **Eigenschaften** für das neu erstellte Richtlinienobjekt anzeigen oder ändern. Damit die Konsole das Dialogfeld **Eigenschaften** anzeigt, wählen Sie die Option **Objekteigenschaften beim Schließen dieses Assistenten anzeigen** auf der letzten Seite des Assistenten „Objekt kopieren – Richtlinienobjekt" aus. Anweisungen bezüglich des Hinzufügens, Änderns und Entfernens von Richtlinien aus einem Richtlinienobjekt finden Sie unter Hinzufügen, Ändern und Entfernen von Richtlinien weiter oben in diesem Dokument.

Umbenennen eines Richtlinienobjekts

Zum Umbenennen eines Richtlinienobjekts klicken Sie mit der rechten Maustaste auf das Richtlinienobjekt und klicken Sie dann auf **Umbenennen**. Geben Sie den neuen Namen ein und drücken Sie dann die Eingabetaste. Das Umbenennen eines Richtlinienobjekts hat keine Auswirkungen auf seine Verknüpfungen. Der Grund ist, dass auf Richtlinienobjekte über unveränderliche Bezeichner statt über ihre Namen verwiesen wird.

Verfahren zum Umbenennen eines Richtlinienobjekts

So benennen Sie ein Richtlinienobjekt um:

1. Wählen Sie in der Konsolenstruktur unter **Configuration | Policies | Administration** den Ordner aus, der das Richtlinienobjekt enthält, das Sie umbenennen möchten.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf das Richtlinienobjekt und klicken Sie dann auf **Umbenennen**.
3. Geben Sie einen neuen Namen ein und drücken Sie dann die Eingabetaste.

Wenn ein Richtlinienobjekt innerhalb von Quest One ActiveRoles angewandt wird, um die Richtlinieneinstellungen im Verzeichnis festzulegen, führt die Umbenennung des Richtlinienobjekts zu keinen Änderungen an den Richtlinieneinstellungen im Verzeichnis. Bei der Anwendung eines Richtlinienobjekts verweist Quest One ActiveRoles mit Hilfe einer internen Kennung und nicht mit Hilfe des Namens des Richtlinienobjekts auf das entsprechende Richtlinienobjekt.

Exportieren und Importieren von Richtlinienobjekten

Mit der Quest One ActiveRoles-Konsole können Sie Richtlinienobjekte in eine XML-Datei exportieren und sie dann aus dieser Datei importieren, um eine andere Instanz von Quest One ActiveRoles aufzufüllen. Die Export- und Importvorgänge stellen eine Möglichkeit bereit, Richtlinienobjekte von einer Testumgebung in eine Produktionsumgebung zu verschieben.

Wenn Sie Richtlinienobjekte erst exportieren und dann importieren, werden nur Richtlinien übertragen. Die Richtlinienobjektverknüpfungen werden in den Export-Import-Vorgang nicht eingeschlossen. Sie müssen sie nach Abschluss des Vorgangs manuell neu konfigurieren.

Um Richtlinienobjekte zu exportieren, wählen Sie sie aus, klicken Sie mit der rechten Maustaste auf die Auswahl und wählen Sie dann **Alle Aufgaben | Exportieren**. Geben Sie im Dialogfeld **Objekte exportieren** die Datei an, in der Sie die Daten speichern möchten, und klicken Sie dann auf **Speichern**.

Zum Importieren von Richtlinienobjekten klicken Sie mit der rechten Maustaste auf den Container, in dem Sie die Richtlinienobjekte ablegen möchten, und klicken Sie dann auf **Importieren**. Wählen Sie im Dialogfeld **Verzeichnisobjekte importieren** die Datei aus, in die die Richtlinienobjekte exportiert wurden, und klicken Sie dann auf **Öffnen**.

Löschen eines Richtlinienobjekts

Um ein Richtlinienobjekt zu löschen, müssen Sie zunächst die Verknüpfungen mit dem Richtlinienobjekt löschen (siehe Verwalten des Richtlinienbereichs weiter oben in diesem Kapitel). Dann können Sie den Löschvorgang wie folgt ausführen: Klicken Sie mit der rechten Maustaste auf das Richtlinienobjekt und klicken Sie dann auf **Löschen**.

Verfahren zum Löschen eines Richtlinienobjekts

So löschen Sie ein Richtlinienobjekt:

1. Wählen Sie in der Konsolenstruktur unter **Configuration | Policies | Administration** den Ordner aus, der das Richtlinienobjekt enthält, das Sie löschen möchten.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf das Richtlinienobjekt und klicken Sie dann auf **Löschen**.

Wenn ein Richtlinienobjekt innerhalb von Quest One ActiveRoles angewandt wird, um Richtlinieneinstellungen im Verzeichnis festzulegen, kann das Richtlinienobjekt nicht gelöscht werden. Sie können eine Liste von Objekten anzeigen, auf die das Richtlinienobjekt angewandt wird: Klicken Sie mit der rechten Maustaste auf das Richtlinienobjekt und klicken Sie dann auf **Richtlinienbereich**. Wenn Sie das Richtlinienobjekt löschen müssen, entfernen Sie zunächst alle Elemente aus der Liste im Dialogfeld **Quest One ActiveRoles-Richtlinienbereich**.

Konfigurationsaufgaben für Richtlinien

In diesem Abschnitt wird beschrieben, wie Sie Richtlinien der folgenden Typen konfigurieren können, gruppiert nach Richtlinienobjektkategorie:

RICHTLINIENOBJEKTKATEGORIE	RICHTLINIENTYP
Bereitstellungsrichtlinienobjekt	Erzeugung und Validierung von Eigenschaften
	Erzeugung von Benutzeranmeldenamen
	Automatische Bereitstellung der Gruppenmitgliedschaft
	E-Mail-Aliaserzeugung
	Automatische Bereitstellung des Exchange-Postfachs
	Stammordner AutoProvisioning
	Skriptausführung
Deprovisionsrichtlinienobjekt	Benutzerkonto-Deprovisionierung
	Entfernung der Gruppenmitgliedschaft
	Exchange-Postfach-Deprovisionierung
	Stammordner-Deprovisionierung
	Benutzerkonto-Verschiebung
	Permanentes Löschen des Benutzerkontos
	Gruppenobjekt-Deprovisionierung
	Gruppenobjekt-Verschiebung
	Dauerhaftes Löschen des Gruppenobjekts
	Benachrichtigungsverteilung
	Berichtsverteilung
	Skriptausführung

Erzeugung und Validierung von Eigenschaften

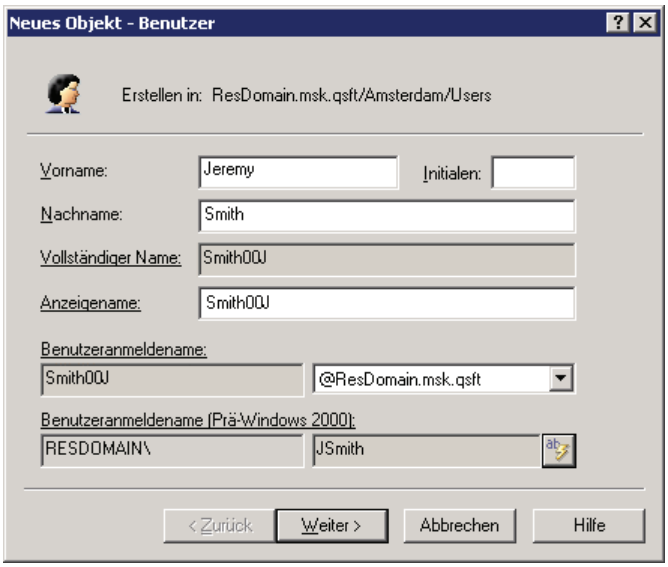
Richtlinien dieser Kategorie dienen zur Generierung von Standardwerten für Eigenschaften bei der Erstellung neuer Verzeichnisobjekte, z.B. Benutzerkonten oder Gruppen. Beim Erstellen oder Ändern von Verzeichnisobjekten wird mit ihnen überprüft, ob Eigenschaftswerte Unternehmensstandards entsprechen.

Sie können für eine beliebige Objekteigenschaft Kriterien angeben, die die Eigenschaftswerte erfüllen müssen, sowie Regeln dafür definieren, welcher Wert der Eigenschaft standardmäßig zugewiesen werden muss. Sie können beispielsweise eine Richtlinie konfigurieren, um eine bestimmte Formatierung von Telefonnummern in Ihrem Verzeichnis durchzusetzen.

Funktionsweise dieser Richtlinie

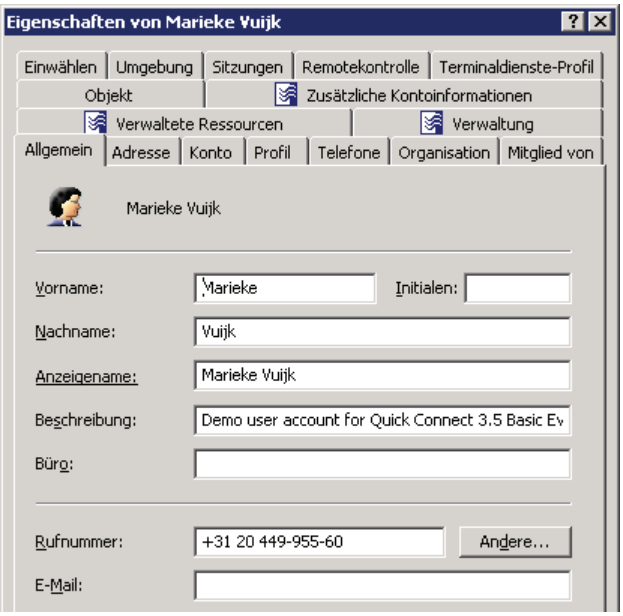
Beim Erstellen oder Ändern eines Objekts überprüft Quest One ActiveRoles, ob die Eigenschaftswerte die in der Richtlinie definierten Kriterien erfüllen. Wenn sie sie nicht erfüllen, verhindert Quest One ActiveRoles die Erstellung oder Änderung des Objekts.

In Objekterstellungsassistenten und Eigenschaftsdialogfeldern werden die Eigenschaften, die von der Richtlinie kontrolliert werden, als Hyperlinks angezeigt. Wenn Sie über eine Richtlinie verfügen, die zum Auffüllen einer Eigenschaft mit einem bestimmten Wert (Generieren des Standardwerts) konfiguriert ist, ist das Bearbeitungsfeld für die Eigenschaft nicht zur Bearbeitung verfügbar, wie in der folgenden Abbildung gezeigt.



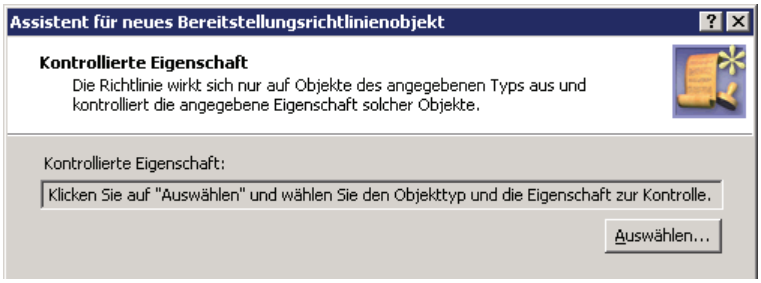
Sie können auf einen Hyperlink klicken, um die Richtliniendetails anzuzeigen.

Wenn eine Richtlinie so konfiguriert ist, dass sie eine Gruppe akzeptabler Werte für eine bestimmte Eigenschaft definiert, stellt die Quest One ActiveRoles-Konsole ein Dropdown-Listenfeld bereit, in dem Sie beim Ändern dieser Eigenschaft einen Wert auswählen können. Der Benutzer der Quest One ActiveRoles-Konsole kann somit einen akzeptablen Wert in der Liste auswählen, statt einen Wert in das Bearbeitungsfeld eingeben zu müssen. Diese Funktion wird in der folgenden Abbildung veranschaulicht: Das Feld **Büro** stellt eine Liste der akzeptablen, von der Richtlinie vorgeschriebenen Werte bereit.

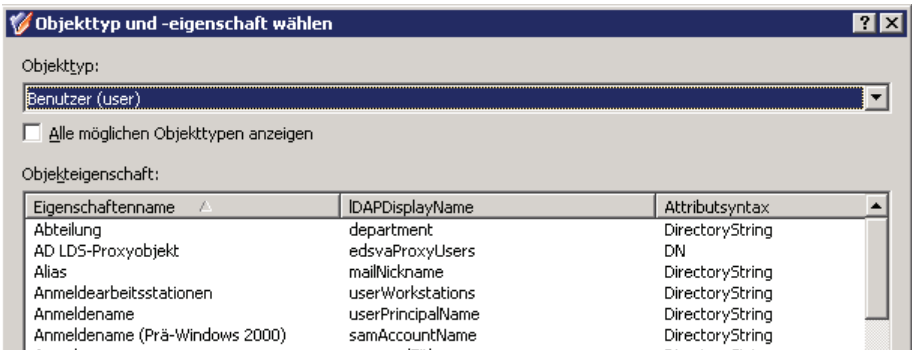


Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften"

Um die Richtlinie „Erzeugung und Validierung von Eigenschaften" zu konfigurieren, wählen Sie **Erzeugung und Validierung von Eigenschaften** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten für neues Bereitstellungsrichtlinienobjekt oder im Assistenten „Bereitstellungsrichtlinie hinzufügen" aus. Klicken Sie dann auf **Weiter**, um die Seite **Kontrollierte Eigenschaft** anzuzeigen:

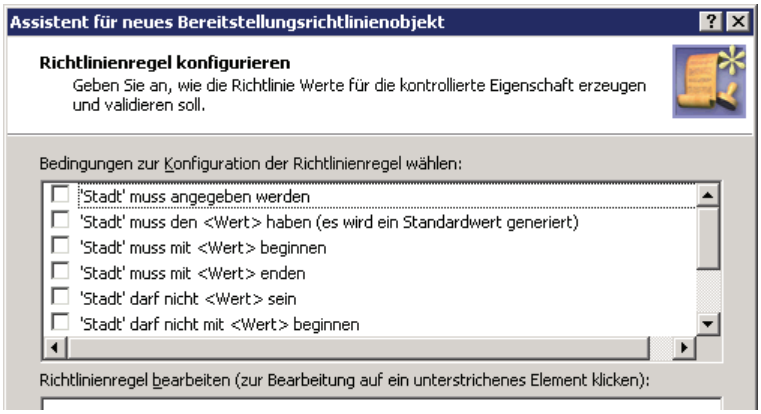

Assistent für neues Bereitstellungsrichtlinienobjekt
Kontrollierte Eigenschaft
Die Richtlinie wirkt sich nur auf Objekte des angegebenen Typs aus und kontrolliert die angegebene Eigenschaft solcher Objekte.
Kontrollierte Eigenschaft:
Klicken Sie auf "Auswählen" und wählen Sie den Objekttyp und die Eigenschaft zur Kontrolle.
Auswählen...

Klicken Sie auf **Auswählen**, um den Objekttyp und die Objekteigenschaft auszuwählen, die die Richtlinie steuern soll. Daraufhin wird das Dialogfeld **Objekttyp und -eigenschaft wählen** angezeigt:



Wählen Sie in der Liste **Objekttyp** den Objekttyp aus: So geben Sie den Typ der Objekte an, die durch die Richtlinie gesteuert werden sollen. Wählen Sie in der Liste **Objekteigenschaft** die Objekteigenschaft aus: So geben Sie die Eigenschaft an, die durch die Richtlinie gesteuert werden soll. Klicken Sie auf **OK**.

Klicken Sie auf der Seite **Kontrollierte Eigenschaft** auf **Weiter**, um die Seite **Richtlinienregel konfigurieren** anzuzeigen:


Assistent für neues Bereitstellungsrichtlinienobjekt
Richtlinienregel konfigurieren
Geben Sie an, wie die Richtlinie Werte für die kontrollierte Eigenschaft erzeugen und validieren soll.
Bedingungen zur Konfiguration der Richtlinienregel wählen:
'Stadt' muss angegeben werden
'Stadt' muss den <Wert> haben (es wird ein Standardwert generiert)
'Stadt' muss mit <Wert> beginnen
'Stadt' muss mit <Wert> enden
'Stadt' darf nicht <Wert> sein
'Stadt' darf nicht mit <Wert> beginnen
Richtlinienregel bearbeiten (zur Bearbeitung auf ein unterstrichenes Element klicken):

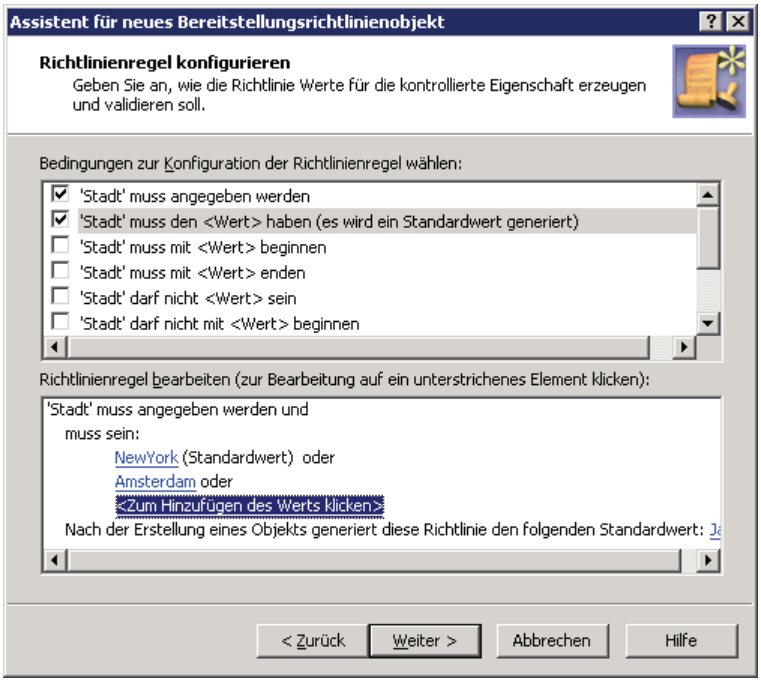
Auf dieser Seite können Sie Kriterien bestimmen, mit denen Werte der gesteuerten Eigenschaft generiert und überprüft werden.

Aktivieren Sie zum Konfigurieren einer Richtlinienregel zunächst die entsprechenden Kontrollkästchen im oberen Feld auf der Seite **Richtlinienregel konfigurieren**. Jede Kontrollkästchenbeschriftung besteht aus dem Namen der gesteuerten Eigenschaft, gefolgt von einer Bedingung. Wenn Sie beispielsweise das Kontrollkästchen neben **muss angegeben werden** aktivieren, setzt die Richtlinie durch, dass der Eigenschaft ein Wert zugewiesen wird.

Wenn die Richtlinie einen Standardwert für die gesteuerte Eigenschaft generieren soll, aktivieren Sie das Kontrollkästchen neben **muss den <Wert> haben (es wird ein Standardwert generiert)**.

Wenn die Richtlinie nicht zwischen Groß- und Kleinschreibung unterscheiden soll, aktivieren Sie das Kontrollkästchen neben **ohne Unterscheidung nach Groß-/Kleinschreibung**.

Nach dem Aktivieren von Kontrollkästchen im oberen Feld werden Sie im unteren Feld zum Konfigurieren von Werten aufgefordert, wie in der folgenden Abbildung gezeigt.


Assistent für neues Bereitstellungsrichtlinienobjekt
Richtlinienregel konfigurieren
Geben Sie an, wie die Richtlinie Werte für die kontrollierte Eigenschaft erzeugen und validieren soll.
Bedingungen zur Konfiguration der Richtlinienregel wählen:
'Stadt' muss angegeben werden
'Stadt' muss den <Wert> haben (es wird ein Standardwert generiert)
'Stadt' muss mit <Wert> beginnen
'Stadt' muss mit <Wert> enden
'Stadt' darf nicht <Wert> sein
'Stadt' darf nicht mit <Wert> beginnen
Richtlinienregel bearbeiten (zur Bearbeitung auf ein unterstrichenes Element klicken):
'Stadt' muss angegeben werden und
muss sein:
NewYork (Standardwert) oder
Amsterdam oder
<Zum Hinzufügen des Werts klicken>
Nach der Erstellung eines Objekts generiert diese Richtlinie den folgenden Standardwert:
< Zurück
Weiter >
Abbrechen
Hilfe

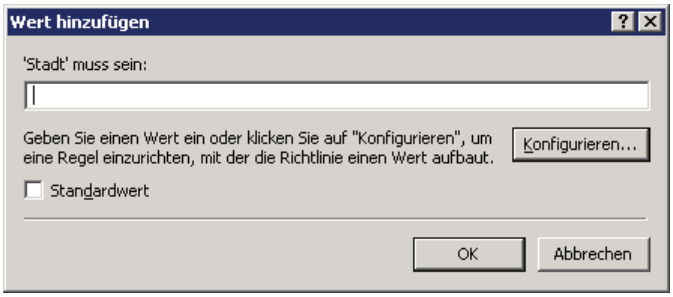
Klicken Sie im unteren Feld auf Verknüpfungen mit der Beschriftung **<Zum Hinzufügen des Werts klicken>**, um weitere Werte zu konfigurieren. Wenn Sie im oberen Feld mehrere Kontrollkästchen aktivieren, müssen Sie für jede Bedingung einen Wert konfigurieren.

Im Feld **Richtlinienregel bearbeiten** können Sie auch die folgenden Aktionen ausführen:

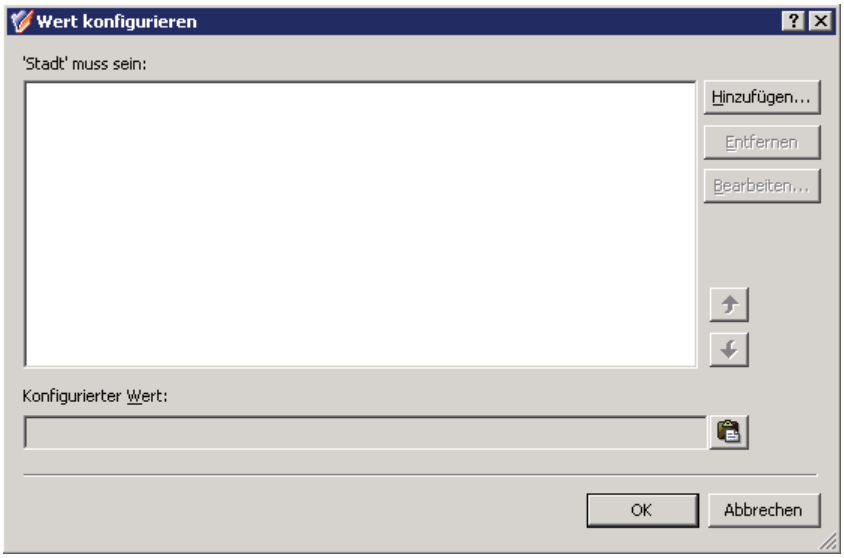
- Ändern eines Wertes. Klicken Sie mit der rechten Maustaste auf den Wert und klicken Sie dann auf **Bearbeiten**. Nun wird ein Dialogfeld ähnlich dem Dialogfeld **Wert hinzufügen** angezeigt, das weiter unten in diesem Abschnitt diskutiert wird.
- Entfernen eines Wertes. Klicken Sie mit der rechten Maustaste auf den Wert und klicken Sie dann auf **Entfernen**.
- Neu anordnen der Werteliste (vorausgesetzt, dass mehrere Werte für eine bestimmte Bedingung angegeben sind). Klicken Sie mit der rechten Maustaste auf einen Wert und verwenden Sie den Befehl **Nach oben** bzw. **Nach unten**, um die Position des Werts in der Liste zu ändern, oder klicken Sie auf **Elemente in aufsteigender Reihenfolge sortieren** bzw. **Elemente in absteigender Reihenfolge sortieren**, um die Liste entsprechend zu sortieren.
- Importieren von Werten aus einer Textdatei. Bereiten Sie eine Textdatei vor, die einen Wert je Zeile enthält, klicken Sie mit der rechten Maustaste auf einen beliebigen Wert im Feld **Richtlinienregel bearbeiten**, klicken Sie auf **Elemente importieren** und öffnen Sie dann die Datei, die Sie vorbereitet haben.
- Exportieren der Werte in eine Textdatei. Klicken Sie mit der rechten Maustaste auf einen beliebigen Wert, klicken Sie auf **Elemente exportieren** und geben Sie eine Textdatei an, in die die Werte geschrieben werden sollen.
- Angeben, ob die Regel den Standardwert generieren soll. Klicken Sie auf die Verknüpfung **Ja** oder **Nein**, um diese Option umzuschalten.

Um Kriterien in der Richtlinienregel zu kombinieren, verwenden Sie die Operatoren UND und ODER. Die Richtlinie wird eingehalten, wenn der Eigenschaftswert alle angegebenen Kriterien bzw. ein beliebiges von ihnen erfüllt. Zum Ändern des Operators klicken Sie auf die Schaltfläche **und** oder **oder**.

Durch Anklicken der Verknüpfung mit dem Namen **<Zum Hinzufügen des Werts klicken>** wird ein Dialogfeld angezeigt, dass dem in der folgenden Abbildung gezeigten Dialogfeld entspricht.


Wert hinzufügen
'Stadt' muss sein:
Geben Sie einen Wert ein oder klicken Sie auf "Konfigurieren", um eine Regel einzurichten, mit der die Richtlinie einen Wert aufbaut.
Konfigurieren...
Standardwert
OK
Abbrechen

Im Dialogfeld **Wert hinzufügen** können Sie einen Wert für die ausgewählte Bedingung angeben. Sie können in das Bearbeitungsfeld einen Wert eingeben oder über die Benutzeroberfläche zum Zeigen und Klicken einen Wert konfigurieren. Durch Anklicken der Schaltfläche **Konfigurieren** wird das Dialogfeld **Wert konfigurieren** angezeigt, das in der folgenden Abbildung dargestellt ist.



Jeder Wert entsteht durch Verkettung von mindestens einem Eintrag. Im Dialogfeld **Wert konfigurieren** können Sie folgende Aktionen ausführen:

- Hinzufügen beliebig vieler Einträge zu dem Wert. Klicken Sie auf **Hinzufügen**, um das Fenster **Eintrag hinzufügen** anzuzeigen, das weiter unten in diesem Abschnitt diskutiert wird.
- Entfernen von Einträgen aus dem Wert. Wählen Sie in der Liste Einträge aus und klicken Sie auf **Entfernen**.
- Ändern von Einträgen im Wert. Wählen Sie einen Eintrag aus und klicken Sie auf **Bearbeiten**. Nun wird ein Fenster angezeigt, das dem Fenster **Eintrag hinzufügen** ähnelt und in dem Sie die Eintragseigenschaften anzeigen und ändern können.

- Verschieben des ausgewählten Eintrags nach oben oder unten in der Liste, um die Einträge in dem Wert anders anzuordnen. Klicken Sie im oberen Feld auf einen Eintrag und klicken Sie dann auf die Schaltflächen mit den Pfeilen neben dem Feld, um den Eintrag zu verschieben.
- Einfügen des Textes aus der Zwischenablage am Ende des Wertes. Wenn der Text eine gültige Syntax aufweist, mit der ein Eintrag eines anderen Typs als **Text** implementiert wird (siehe Tabelle unten), wird die Syntax entsprechend behandelt. Kopieren Sie einen Text in die Zwischenablage und klicken Sie dann auf die Schaltfläche neben dem Feld **Konfigurierter Wert**, um den Text hinter das Ende der Zeichenfolge in diesem Feld einzufügen.

Im Fenster **Eintrag hinzufügen** können Sie den Typ des hinzuzufügenden Eintrags auswählen und den Eintrag dann konfigurieren. In der folgenden Tabelle werden die verfügbaren Eintragstypen zusammengefasst.

EINTRAGSTYP	BESCHREIBUNG
Text	Fügt dem Wert eine Textzeichenfolge hinzu.
<*Objekt*>eigenschaft	Fügt eine ausgewählte Eigenschaft des von der Richtlinie verwalteten Objekts (oder einen Teil einer Eigenschaft) hinzu. Wenn ein Eintrag dieses Typs angezeigt wird, ersetzt die Konsole den Platzhalter <*Objekt*> durch die tatsächliche Kategorie der Objekte, die der Steuerung der Richtlinie unterliegen. Wenn die Richtlinie beispielsweise für die Steuerung einer bestimmten Eigenschaft von Benutzerobjekten konfiguriert ist, können Sie mit Hilfe von Einträgen dieses Typs diese Eigenschaft eines Benutzerobjekts mit Daten aus anderen Eigenschaften des gleichen Benutzerobjekts auffüllen.
Eigenschaft der übergeordneten Organisationseinheit	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) einer Organisationseinheit in der Containerhierarchie über dem von dieser Richtlinie verwalteten Objekt hinzu. Wenn die Richtlinie beispielsweise für die Steuerung einer bestimmten Eigenschaft von Benutzerobjekten konfiguriert ist, können Sie mit Hilfe von Einträgen dieses Typs diese Eigenschaft eines Benutzerobjekts mit Daten aus Eigenschaften der Organisationseinheit auffüllen, die dieses Benutzerobjekt enthält (also der unmittelbar übergeordneten Organisationseinheit).
Eigenschaft der übergeordneten Domäne	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) der Domäne des von dieser Richtlinie verwalteten Objekts hinzu. Wenn die Richtlinie beispielsweise für die Steuerung einer bestimmten Eigenschaft von Benutzerobjekten konfiguriert ist, können Sie mit Hilfe von Einträgen dieses Typs diese Eigenschaft eines Benutzerobjekts mit Daten auffüllen, die in Eigenschaften der Domäne gespeichert sind, in der sich dieses Benutzerobjekt befindet.
Maske	Fügt eine Syntax hinzu, die bestimmt, welche Zeichen in der von dieser Richtlinie gesteuerten Eigenschaft zulässig sind. Mit Einträgen dieses Typs können Sie ein Datenformat durchsetzen, beispielsweise für Zahlen, Postleitzahlen oder Telefonnummern.

Die Schritte zum Konfigurieren eines Eintrags hängen vom Eintragstyp ab. In den folgenden Abschnitten werden die Vorgehensweisen für jeden der Eintragstypen näher beschrieben, die im Fenster **Eintrag hinzufügen** vorkommen.

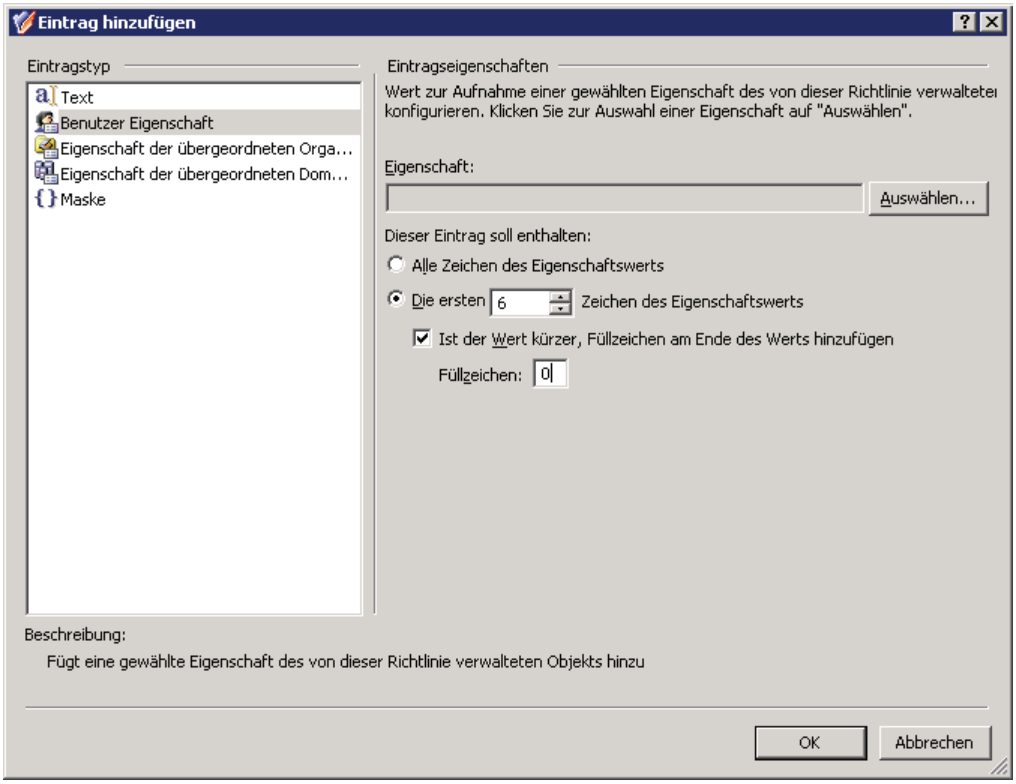
Eintragstyp: Text

Wenn Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** den Typ **Text** auswählen, wird im Bereich **Eintragseigenschaften** das Feld **Textwert** angezeigt.

Geben Sie in das Feld **Textwert** den Text ein, den Sie in den Wert einschließen möchten, und klicken Sie dann auf **OK**.

Eintragstyp: <Objekt>eigenschaft

Wenn Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** den Typ **<Objekt> Eigenschaft** auswählen, ähnelt der Bereich **Eintragseigenschaften** der folgenden Abbildung.



Mit diesem Eintragstyp können Sie einen Wert konfigurieren, der auf einer Eigenschaft des Objekts selbst basiert. Um eine Eigenschaft auszuwählen, klicken Sie auf **Auswählen**.

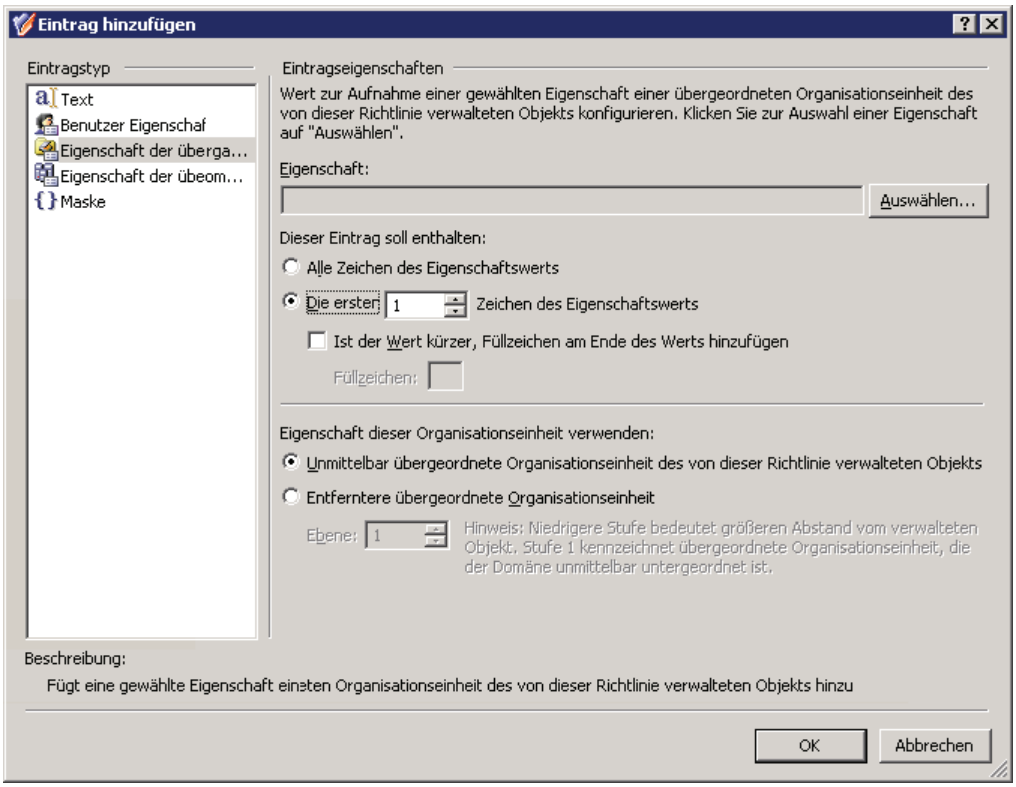
Wenn der Eintrag den gesamten Wert der Eigenschaft enthalten soll, klicken Sie auf **Alle Zeichen des Eigenschaftswerts**. Klicken Sie andernfalls auf **Die ersten** und geben Sie an, wie viele Zeichen in den Eintrag eingeschlossen werden sollen.

Im letzteren Fall können Sie das Kontrollkästchen **Ist der Wert kürzer, Füllzeichen am Ende des Werts hinzufügen** aktivieren und ein Zeichen in das Feld **Füllzeichen** eingeben. Dieses Zeichen ersetzt die fehlenden Zeichen im Wert der Objekteigenschaft, wenn dieser Wert kürzer ist als im Feld neben der Option **Die ersten** angegeben.

Klicken Sie nach dem Konfigurieren eines Eintrags auf **OK**, um das Fenster **Eintrag hinzufügen** zu schließen. Der Eintrag wird dem Dialogfeld **Wert konfigurieren** hinzugefügt.

Eintragstyp: Eigenschaft der übergeordneten Organisationseinheit

Wenn Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** den Typ **Eigenschaft der übergeordneten Organisationseinheit** auswählen, ähnelt der Bereich **Eintragseigenschaften** der folgenden Abbildung.


Eintrag hinzufügen
Eintragstyp
Text
Benutzer Eigenschaf
Eigenschaft der überga...
Eigenschaft der übeom...
Maske
Eintragseigenschaften
Wert zur Aufnahme einer gewählten Eigenschaft einer übergeordneten Organisationseinheit des von dieser Richtlinie verwalteten Objekts konfigurieren. Klicken Sie zur Auswahl einer Eigenschaft auf "Auswählen".
Eigenschaft:
Auswählen...
Dieser Eintrag soll enthalten:
Alle Zeichen des Eigenschaftswerts
Die ersten 1 Zeichen des Eigenschaftswerts
Ist der Wert kürzer, Füllzeichen am Ende des Werts hinzufügen
Füllzeichen:
Eigenschaft dieser Organisationseinheit verwenden:
Unmittelbar übergeordnete Organisationseinheit des von dieser Richtlinie verwalteten Objekts
Entferntere übergeordnete Organisationseinheit
Ebene: 1
Hinweis: Niedrigere Stufe bedeutet größeren Abstand vom verwalteten Objekt. Stufe 1 kennzeichnet übergeordnete Organisationseinheit, die der Domäne unmittelbar untergeordnet ist.
Beschreibung:
Fügt eine gewählte Eigenschaft einsten Organisationseinheit des von dieser Richtlinie verwalteten Objekts hinzu
OK
Abbrechen

Mit diesem Eintragstyp können Sie einen Wert konfigurieren, der auf einer Eigenschaft einer übergeordneten Organisationseinheit des von dieser Richtlinie verwalteten Objekts basiert. Um eine Eigenschaft einer Organisationseinheit auszuwählen, klicken Sie auf **Auswählen**.

Wenn der Eintrag den gesamten Wert der Eigenschaft enthalten soll, klicken Sie auf **Alle Zeichen des Eigenschaftswerts**. Klicken Sie andernfalls auf **Die ersten** und geben Sie an, wie viele Zeichen in den Eintrag eingeschlossen werden sollen.

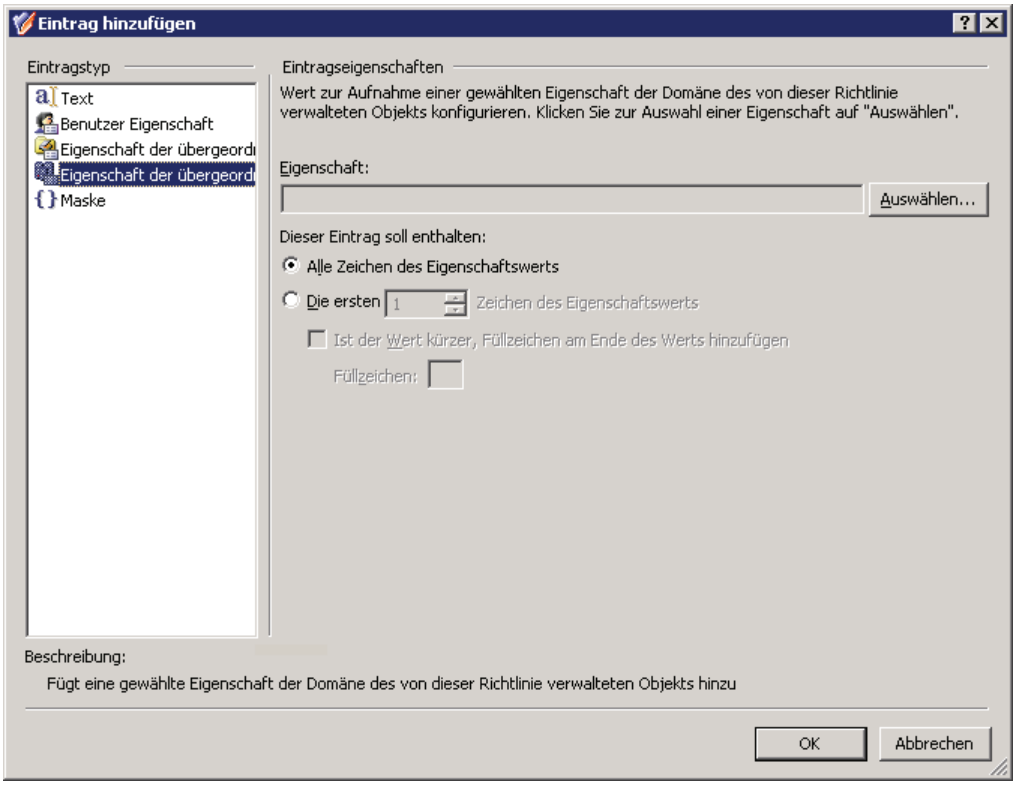
Im letzteren Fall können Sie das Kontrollkästchen **Ist der Wert kürzer, Füllzeichen am Ende des Werts hinzufügen** aktivieren und ein Zeichen in das Feld **Füllzeichen** eingeben. Dieses Zeichen ersetzt die fehlenden Zeichen im Wert der Organisationseinheitseigenschaft, wenn dieser Wert kürzer ist als im Feld neben der Option **Die ersten** angegeben.

Sie können auch die Ebene der Organisationseinheit angeben, die von der Richtlinie verwendet werden soll. Um die Eigenschaft der Organisationseinheit zu verwenden, in der sich das Objekt befindet, klicken Sie auf **Unmittelbar übergeordnete Organisationseinheit des von dieser Richtlinie verwalteten Objekts**. Um die Eigenschaft einer übergeordneten Organisationseinheit einer anderen Ebene zu verwenden, klicken Sie auf **Entferntere übergeordnete Organisationseinheit**, und geben Sie dann im Feld **Ebene** die Ebene der Organisationseinheit an. Eine tiefere Ebene bedeutet eine größere Entfernung vom verwalteten Objekt in der Containerhierarchie über diesem Objekt. Die Ebene 1 bedeutet eine unmittelbar untergeordnete Organisationseinheit der Domäne.

Klicken Sie nach dem Konfigurieren eines Eintrags auf **OK**, um das Fenster **Eintrag hinzufügen** zu schließen. Der Eintrag wird dem Dialogfeld **Wert konfigurieren** hinzugefügt.

Eintragstyp: Eigenschaft der übergeordneten Domäne

Wenn Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** den Typ **Eigenschaft der übergeordneten Domäne** auswählen, ähnelt der Bereich **Eintragseigenschaften** der folgenden Abbildung.


Eintrag hinzufügen
Eintragstyp
Text
Benutzer Eigenschaft
Eigenschaft der übergeordn
Eigenschaft der übergeordn
Maske
Eintragseigenschaften
Wert zur Aufnahme einer gewählten Eigenschaft der Domäne des von dieser Richtlinie verwalteten Objekts konfigurieren. Klicken Sie zur Auswahl einer Eigenschaft auf "Auswählen".
Eigenschaft:
Auswählen...
Dieser Eintrag soll enthalten:
Alle Zeichen des Eigenschaftswerts
Die ersten 1 Zeichen des Eigenschaftswerts
Ist der Wert kürzer, Füllzeichen am Ende des Werts hinzufügen
Füllzeichen:
Beschreibung:
Fügt eine gewählte Eigenschaft der Domäne des von dieser Richtlinie verwalteten Objekts hinzu
OK
Abbrechen

Mit diesem Eintragstyp können Sie einen Wert konfigurieren, der auf einer Eigenschaft der Domäne des von dieser Richtlinie verwalteten Objekts basiert. Um eine Domäneneigenschaft auszuwählen, klicken Sie auf **Auswählen**.

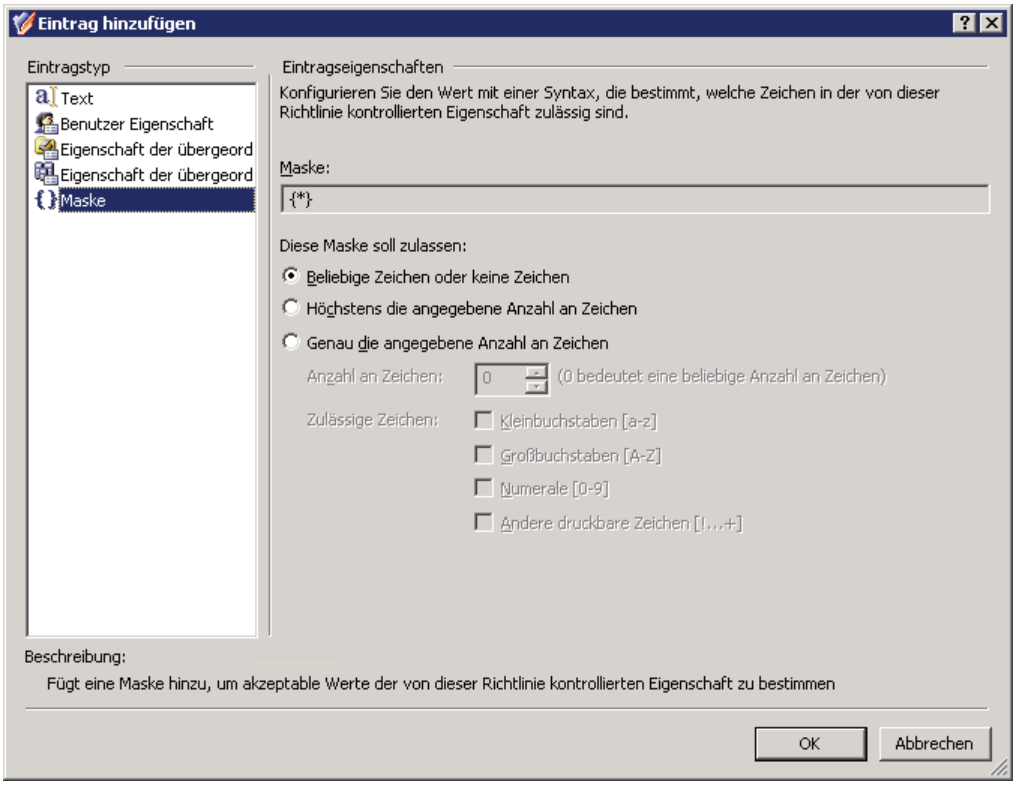
Wenn der Eintrag den gesamten Wert der Eigenschaft enthalten soll, klicken Sie auf **Alle Zeichen des Eigenschaftswerts**. Klicken Sie andernfalls auf **Die ersten** und geben Sie an, wie viele Zeichen in den Eintrag eingeschlossen werden sollen.

Im letzteren Fall können Sie das Kontrollkästchen **Ist der Wert kürzer, Füllzeichen am Ende des Werts hinzufügen** aktivieren und ein Zeichen in das Feld **Füllzeichen** eingeben. Dieses Zeichen ersetzt die fehlenden Zeichen im Wert der Domäneneigenschaft, wenn dieser Wert kürzer ist als im Feld neben der Option **Die ersten** angegeben.

Klicken Sie nach dem Konfigurieren eines Eintrags auf **OK**, um das Fenster **Eintrag hinzufügen** zu schließen. Der Eintrag wird dem Dialogfeld **Wert konfigurieren** hinzugefügt.

Eintragstyp: Maske

Wenn Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** den Typ **Maske** auswählen, ähnelt der Bereich **Eintragseigenschaften** der folgenden Abbildung.



Mit diesem Eintragstyp können Sie definieren, welche Zeichen (Buchstaben, Ziffern) in dem Eintrag zulässig sind, den Sie dem Wert der gesteuerten Eigenschaft hinzufügen.

Wenn Sie für den Eintrag beliebige Folgen von Zeichen zulassen möchten, klicken Sie auf **Beliebige Zeichen oder keine Zeichen**.

Wenn Sie eine Maximalzahl zulässiger Zeichen im Eintrag angeben möchten, klicken Sie auf **Höchstens die angegebene Anzahl an Zeichen**. Geben Sie im Feld **Anzahl an Zeichen** die Anzahl zulässiger Zeichen an. Der Eintrag kann beliebig viele Zeichen bis hin zur angegebenen Anzahl enthalten. Aktivieren Sie unter **Zulässige Zeichen** Kontrollkästchen, um die zulässigen Zeichen anzugeben.

Wenn Sie eine genaue Anzahl im Eintrag erforderlicher Zeichen angeben möchten, klicken Sie auf **Genau die angegebene Anzahl an Zeichen**. Geben Sie im Feld **Anzahl an Zeichen** die Anzahl zulässiger Zeichen an. Der Eintrag muss genau die angegebene Anzahl von Zeichen enthalten. Aktivieren Sie unter **Zulässige Zeichen** Kontrollkästchen, um die zulässigen Zeichen anzugeben.

Klicken Sie nach dem Konfigurieren eines Eintrags auf **OK**, um das Fenster **Eintrag hinzufügen** zu schließen. Der Eintrag wird dem Dialogfeld **Wert konfigurieren** hinzugefügt.

Verfahren zum Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften"

So konfigurieren Sie eine Richtlinie für die Erzeugung und Validierung von Eigenschaften:

1. Wählen Sie auf der Seite **Zu konfigurierende Richtlinie** die Option **Erzeugung und Validierung von Eigenschaften** aus und klicken Sie dann auf **Weiter**.
2. Klicken Sie auf **Wählen**, um den Objekttyp und die Objekteigenschaft auszuwählen, die die Richtlinie steuern soll.
3. Vervollständigen Sie das Dialogfeld **Objekttyp und eigenschaft wählen**, indem Sie das weiter unten in diesem Thema beschriebene Verfahren befolgen, und klicken Sie dann auf **Weiter**.
4. Gehen Sie auf der Seite **Richtlinienregel konfigurieren** wie nachfolgend beschrieben vor und klicken Sie dann auf **Weiter**:
   - Aktivieren Sie die entsprechenden Kontrollkästchen zur Konfiguration der Regel.
   - Klicken Sie im unteren Bereich auf die Verknüpfungen ***Zum Hinzufügen des Werts klicken*** und vervollständigen Sie das Dialogfeld **Wert hinzufügen**, indem Sie das weiter unten in diesem Thema beschriebene Verfahren befolgen.
   - Um zwischen UND und ODER zu wechseln, klicken Sie auf ***und*** oder ***oder***.
5. Auf der Seite **Richtlinienbeschreibung** können Sie die Richtlinienbeschreibung ändern:
   - Wählen Sie **Diese Richtlinienbeschreibung ändern** und nehmen Sie bei Bedarf Änderungen an der Richtlinienbeschreibung vor. Klicken Sie dann auf **Weiter**.
6. Auf der Seite **Richtlinie erzwingen** können Sie Objekte angeben, auf die dieses Richtlinienobjekt angewandt werden soll:
   - Klicken Sie auf **Hinzufügen** und verwenden Sie das Objekt **Objekte auswählen**, um die gewünschten Objekte auszuwählen.
7. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Gehen Sie folgendermaßen vor, um das Dialogfeld „Objekttyp und eigenschaft auswählen" abzuschließen:

1. Wählen Sie in der Liste **Objekttyp** den Objekttyp aus, den die Richtlinie beeinflussen soll.
2. Wählen Sie in der Liste **Objekteigenschaft** die Objekteigenschaft aus, die die Richtlinie kontrollieren soll.

   *Wenn die benötigte Eigenschaft nicht angezeigt wird, wählen Sie **Alle mögliche Eigenschaften anzeigen**.*
3. Klicken Sie auf **OK**.

Gehen Sie folgendermaßen vor, um das Dialogfeld „Wert hinzufügen" abzuschließen:

1. Geben Sie einen Wert ein und klicken auf **OK**.

   – ODER –

   Klicken Sie auf **Konfigurieren** und folgen den nächsten Schritten.
2. Klicken Sie auf **Hinzufügen**.
3. Konfigurieren Sie einen Eintrag, in den der Wert aufgenommen werden soll (Anweisungen finden Sie unter Verfahren zum Konfigurieren von Einträgen).
4. Im Dialogfeld **Wert konfigurieren** fügen Sie Einträge hinzu, löschen oder bearbeiten vorhandene Einträge und klicken dann auf **OK**.
5. Aktivieren Sie im Dialogfeld **Wert hinzufügen** das Kontrollkästchen **Standardwert**, wenn der Wert als Standardwert markiert werden soll, und klicken Sie dann auf **OK**.

Verfahren zum Konfigurieren von Einträgen

Gehen Sie gemäß den nachfolgend aufgeführten schrittweisen Anweisungen vor, um einen Eintrag im Dialogfeld **Eintrag hinzufügen** zu konfigurieren. Dieselben Anweisungen gelten, wenn Sie Änderungen an einem vorhandenen Eintrag vornehmen.

Gehen Sie folgendermaßen vor, um einen Texteintrag zu konfigurieren:

1. Klicken Sie unter **Eintragstyp** auf **Text**.

   *Verwenden Sie einen **Texteintrag**, um eine Zeichenkette zu dem Wert hinzuzufügen, den Sie konfigurieren.*

2. Geben Sie im Feld **Textwert** die Zeichenkette ein, die der Wert enthalten soll.
3. Klicken Sie auf **OK**.

Gehen Sie folgendermaßen vor, um einen Eintrag des Typs „<Objekt> Eigenschaft" zu konfigurieren:

1. Klicken Sie unter **Eintragstyp** auf ***<Objekt>* Eigenschaft**.

   *Verwenden Sie einen Eintrag des Typs **<Objekt> Eigenschaft**, wenn Sie einen Wert so konfigurieren möchten, dass er eine bestimmte Eigenschaft (oder einen Teil einer Eigenschaft) des Objekts enthalten soll, der unter der Kontrolle der Richtlinie steht. In diesen Anweisungen steht **<Objekt>** für den Objekttyp wie etwa **Benutzer**, **Gruppe** oder **Computer**.*

2. Klicken Sie auf **Wählen**, klicken Sie dann auf die Eigenschaft, die in den Wert aufgenommen werden soll, und klicken Sie dann auf **OK**.
3. Wenn der Eintrag den gesamten Wert der Eigenschaft enthalten soll, klicken Sie auf **Alle Zeichen des Eigenschaftswerts**. Klicken Sie andernfalls auf **Die ersten** und geben Sie an, wie viele Zeichen in den Eintrag eingeschlossen werden sollen.
4. Wenn Sie **Die ersten** ausgewählt haben, dann wählen Sie optional **Ist der Wert kürzer, Füllzeichen am Ende des Werts hinzufügen** aus und geben Sie ein Zeichen in das Feld **Füllzeichen** ein.

   *Dieses Zeichen ersetzt die fehlenden Zeichen im Wert der Eigenschaft, wenn dieser Wert kürzer ist als im Feld neben der Option **Die ersten** angegeben.*

5. Klicken Sie auf **OK**.

Gehen Sie folgendermaßen vor, um einen Eintrag des Typs „Eigenschaft der übergeordneten Organisationseinheit" zu konfigurieren:

1. Klicken Sie unter **Eintragstyp** auf **Eigenschaft der übergeordneten Organisationseinheit**.

   *Verwenden Sie einen Eintrag des Typs **Eigenschaft der übergeordneten Organisationseinheit**, wenn Sie einen Wert so konfigurieren möchten, dass er eine bestimmte Eigenschaft (oder einen Teil einer Eigenschaft) einer Organisationseinheit in der Hierarchie der Container über dem von der Richtlinie verwalteten Objekt enthalten soll.*

2. Klicken Sie auf **Wählen**, klicken Sie dann auf die Eigenschaft, die in den Wert aufgenommen werden soll, und klicken Sie dann auf **OK**.
3. Wenn der Eintrag den gesamten Wert der Eigenschaft enthalten soll, klicken Sie auf **Alle Zeichen des Eigenschaftswerts**. Klicken Sie andernfalls auf **Die ersten** und geben Sie an, wie viele Zeichen in den Eintrag eingeschlossen werden sollen.
4. Wenn Sie **Die ersten** ausgewählt haben, dann wählen Sie optional **Ist der Wert kürzer, Füllzeichen am Ende des Werts hinzufügen** aus und geben Sie ein Zeichen in das Feld **Füllzeichen** ein.

   *Dieses Zeichen ersetzt die fehlenden Zeichen im Wert der Eigenschaft, wenn dieser Wert kürzer ist als im Feld neben der Option **Die ersten** angegeben.*

5. Wählen Sie eine dieser Optionen aus:
   - Um die Eigenschaft der Organisationseinheit zu verwenden, in der sich das Objekt befindet, klicken Sie auf **Unmittelbar übergeordnete Organisationseinheit des von dieser Richtlinie verwalteten Objekts**.
   - Um die Eigenschaft einer übergeordneten Organisationseinheit einer anderen Ebene zu verwenden, klicken Sie auf **Entferntere übergeordnete Organisationseinheit** und geben Sie dann im Feld **Ebene** die Ebene der Organisationseinheit an.

   Eine tiefere Ebene bedeutet eine größere Entfernung vom verwalteten Objekt in der Containerhierarchie über diesem Objekt. Die Ebene 1 bedeutet eine unmittelbar untergeordnete Organisationseinheit der Domäne.
6. Klicken Sie auf **OK**.

Gehen Sie folgendermaßen vor, um einen Eintrag des Typs „Eigenschaft der übergeordneten Domäne" zu konfigurieren:

1. Klicken Sie unter **Eintragstyp** auf **Eigenschaft der übergeordneten Domäne**.

   *Verwenden Sie einen Eintrag des Typs **Eigenschaft der übergeordneten Domäne**, wenn Sie einen Wert so konfigurieren möchten, dass er eine bestimmte Eigenschaft (oder einen Teil einer Eigenschaft) der Domäne des Objekts enthalten soll, das von der Richtlinie verwaltet wird.*
2. Klicken Sie auf **Wählen**, klicken Sie dann auf die Eigenschaft, die in den Wert aufgenommen werden soll, und klicken Sie dann auf **OK**.
3. Wenn der Eintrag den gesamten Wert der Eigenschaft enthalten soll, klicken Sie auf **Alle Zeichen des Eigenschaftswerts**. Klicken Sie andernfalls auf **Die ersten** und geben Sie an, wie viele Zeichen in den Eintrag eingeschlossen werden sollen.
4. Wenn Sie **Die ersten** ausgewählt haben, dann wählen Sie optional **Ist der Wert kürzer, Füllzeichen am Ende des Werts hinzufügen** aus und geben Sie ein Zeichen in das Feld **Füllzeichen** ein.

   *Dieses Zeichen ersetzt die fehlenden Zeichen im Wert der Eigenschaft, wenn dieser Wert kürzer ist als im Feld neben der Option **Die ersten** angegeben.*
5. Klicken Sie auf **OK**.

Gehen Sie folgendermaßen vor, um einen Eintrag des Typs „Maske" zu konfigurieren:

1. Klicken Sie unter **Eintragstyp** auf **Maske**.

   *Verwenden Sie einen Eintrag des Typs **Maske**, wenn Sie einen Wert so konfigurieren möchten, dass er eine Syntax enthält, die festlegt, wie viele und welche Zeichen in der von der Richtlinie kontrollierten Eigenschaft zulässig sind.*
2. Wählen Sie eine der folgenden Optionen aus:
   - **Beliebige Zeichen oder keine Zeichen**, wenn Sie für den Eintrag beliebige Folgen von Zeichen zulassen möchten.
   - **Höchstens die angegebene Anzahl an Zeichen** , wenn Sie eine Maximalzahl zulässiger Zeichen im Eintrag angeben möchten.
   - **Genau die angegebene Anzahl an Zeichen**, wenn Sie eine genaue Anzahl zulässiger Zeichen angeben möchten, die der Eintrag enthalten muss.
3. Führen Sie eine der folgenden Aktionen aus, wenn Sie die zweite oder dritte Option in Schritt 2 ausgewählt haben:
   - In **Anzahl Zeichen** geben Sie an, wie viele Zeichen in diesem Eintrag zulässig sind.

   Wenn Sie die zweite Option ausgewählt haben, kann der Eintrag jede beliebige Anzahl Zeichen enthalten, darf jedoch nicht die angegebene Anzahl überschreiten.

Wenn Sie die dritte Option ausgewählt haben, muss der Eintrag genau die angegebene Anzahl an Zeichen enthalten.

- Aktivieren Sie unter **Zulässige Zeichen** Kontrollkästchen, um anzugeben, welche Zeichen in diesem Eintrag zulässig sind.

4. Klicken Sie auf **OK**.

Gehen Sie folgendermaßen vor, um einen Eintrag des Typs „Datum und Uhrzeit" zu konfigurieren:

1. Klicken Sie unter **Eintragstyp** auf **Datum und Uhrzeit**.

   *Verwenden Sie einen Eintrag des Typs **Datum und Uhrzeit**, wenn Sie einen Wert so konfigurieren, dass er das Datum und die Uhrzeit des von der Richtlinie durchgeführten Vorgangs enthalten soll (zum Beispiel das Datum und die Uhrzeit, wann der Benutzer deprovisioniert wurde).*

2. Klicken Sie in der Liste unter **Datums- und Zeitformat** auf das gewünschte Datums- oder Uhrzeitformat.
3. Klicken Sie auf **OK**.

Gehen Sie folgendermaßen vor, um einen Eintrag des Typs „Initiator-ID" zu konfigurieren:

1. Klicken Sie unter **Eintragstyp** auf **Initiator-ID**.

   *Verwenden Sie einen Eintrag des Typs **Initiator-ID**, wenn Sie einen Wert so konfigurieren, dass er die ID des Initiators enthalten soll, d. h. der Benutzer, der den von dieser Richtlinie durchgeführten Vorgang initiiert hat (zum Beispiel die ID des Benutzers, der den Deprovisionierungsvorgang initiiert hat). Sie können die Initiator-ID anhand einer Kombination von Eigenschaften des Initiators erstellen.*

2. Wählen Sie eine der folgenden Optionen aus:
   - **Benutzer-Anmeldename (Prä-Windows 2000) des Initiators im Format Domäne\Name**, um die Initiator-ID auf den Prä-Windows 2000-Benutzeranmeldenamen des Initiators zu setzen.
   - **Benutzer-Anmeldename des Initiators**, um die Initiator-ID auf den Benutzeranmeldenamen des Initiators zu setzen.
   - **Initiator-ID anhand einer benutzerdefinierten Regel aufgebaut**, um die Initiator-ID anhand von anderen Initiator-spezifischen Eigenschaften erstellen.
3. Wenn Sie die dritte Option in Schritt 2 ausgewählt haben, klicken Sie auf **Konfigurieren** und verwenden Sie das Dialogfeld **Wert konfigurieren**, um den Wert zu konfigurieren, der als Initiator-ID verwendet werden soll: Klicken Sie auf **Hinzufügen** und geben Sie die Einträge für den Wert an.

   *Sie können Einträge der folgenden Kategorien konfigurieren: **Text** (jede Textzeichenkette), **Initiatoreigenschaft** (eine bestimmte Eigenschaft des Benutzerobjekts „Initiator"), **Eigenschaft der übergeordneten Organisationseinheit** (eine bestimmte Eigenschaft einer Organisationseinheit, die das Benutzerobjekt „Initiator" umfasst), **Eigenschaft der übergeordneten Domäne** (eine bestimmte Eigenschaft der Domäne des Benutzerobjekts „Initiator"). Um diese Einträge zu konfigurieren, gehen Sie gemäß den weiter oben in diesem Hilfethema aufgeführten Anweisungen vor.*

4. Klicken Sie auf **OK**.

Gehen Sie folgendermaßen vor, um einen Eintrag des Typs „Eindeutigkeitszahl" zu konfigurieren:

1. Klicken Sie unter **Eintragstyp** auf **Eindeutigkeitszahl**.

   *Verwenden Sie einen Eintrag des Typs **Eindeutigkeitszahl**, wenn Sie einen Wert konfigurieren möchten, der eine Zahl enthält, die die Richtlinie bei einem Namenskonflikt inkrementieren soll. Sie können zum Beispiel in einer Richtlinie, die einen Benutzeranmeldenamen oder E-Mail-Alias generiert, einen Eintrag dieser Kategorie zur Generierungsregel hinzufügen, um die Eindeutigkeit des von der Richtlinie generierten Namens oder Alias zu gewährleisten.*

2. Klicken Sie auf eine dieser Optionen:
   - **Immer hinzufügen.** Der Wert schließt diesen Eintrag unabhängig davon ein, ob die Richtlinie bei der Anwendung der Generierungsregel einen Namenskonflikt erkennt.
   - **Hinzufügen, wenn Eigenschaftswert in Gebrauch ist.** Die Richtlinie fügt diesen Eintrag bei einem Namenskonflikt zum Wert hinzu; ansonsten enthält dieser Wert nicht diesen Eintrag.
3. Legen Sie fest, wie der Eintrag formatiert werden soll.
   - Damit er als Ziffernfolge variabler Länge formatiert wird, deaktivieren Sie das Kontrollkästchen **Zahl mit fester Länge und voranstehenden Nullen**. In den meisten Fällen ergibt dies einen Eintrag aus nur einer Ziffer.
   - Damit der Eintrag als Ziffernfolge fester Länge formatiert wird, aktivieren Sie das Kontrollkästchen **Zahl mit fester Länge und voranstehenden Nullen** und geben Sie dann die gewünschte Ziffernanzahl ein. Dies generiert einen Eintrag mit der passenden Anzahl von Nullen als Präfix, z.B. 001, 002, 003.
4. Klicken Sie auf **OK**.

- Möglicherweise müssen Sie einen Eintrag konfigurieren, wenn Sie eine Richtlinie wie etwa „Eigenschaftsgenerierung und Bestätigung" (siehe Verfahren zum Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften"), „Generierung eines Benutzeranmeldenamens" (siehe Verfahren zum Konfigurieren einer Richtlinie bezüglich der Generierung eines Benutzeranmeldenamens), „Automatische Bereitstellung der Gruppenmitgliedschaft" (siehe Verfahren zum Konfigurieren der Richtlinie „Automatische Bereitstellung der Gruppenmitgliedschaft"), „E-Mail-Alias-Generierung" (siehe)Verfahren zum Konfigurieren der Richtlinie „E-Mail-Aliaserzeugung", „Benutzerkonto-Deprovisionierung" (siehe Verfahren zum Konfigurieren einer Benutzerkonto-Deprovisionierungsrichtlinie) oder „Gruppenobjekt-Deprovisionierung" (siehe Verfahren zum Konfigurieren einer Gruppenobjekt-Deprovisionierungsrichtlinie) konfigurieren.
- Der Inhalt der Liste **Eintragstyp** im Dialogfeld **Eintrag hinzufügen** ist vom Typ der Richtlinie abhängig, die Sie konfigurieren.

Szenario 1: Durchsetzen eines Formats für Telefonnummern mit Hilfe einer Maske

In diesem Szenario wird beschrieben, wie Sie eine Richtlinie konfigurieren, die für die Telefonnummern von Benutzern das Format (###) ###-##-## durchsetzt.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie ein Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Folglich überprüft Quest One ActiveRoles beim Erstellen oder Ändern eines Benutzerobjekts in dem in Schritt 2 ausgewählten Container, ob die Telefonnummer dem angegebenen Format entspricht. Wenn sie ihm nicht entspricht, verbietet die Richtlinie die Erstellung oder Änderung des Benutzerobjekts.

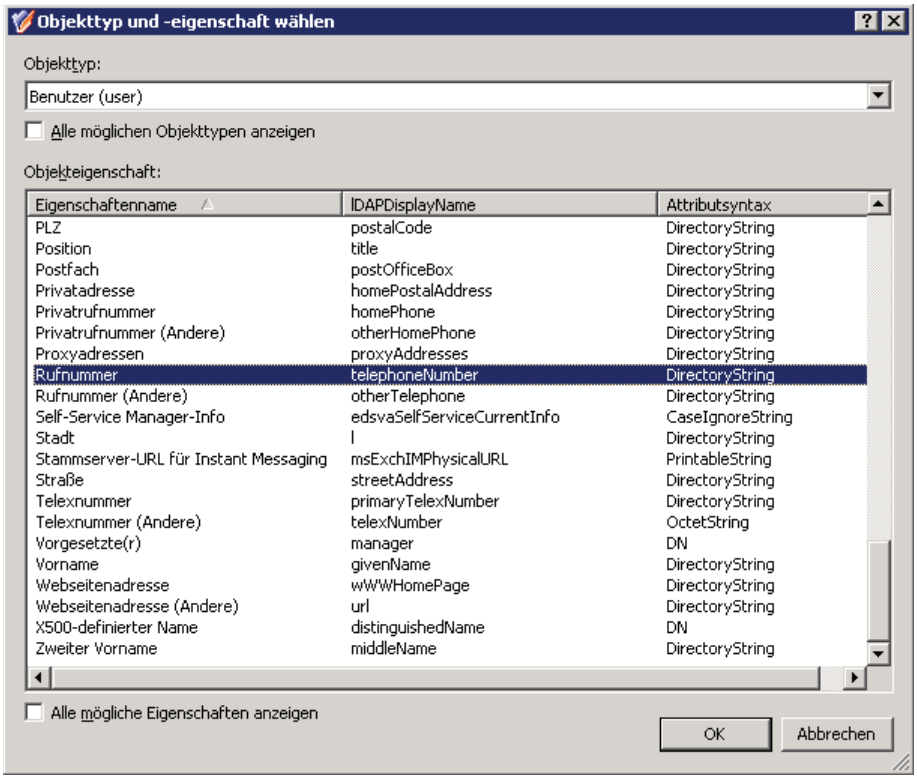
In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten für neues Bereitstellungsrichtlinienobjekt erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter Erstellen eines Richtlinienobjekts im Abschnitt Verwaltungsaufgaben für Richtlinienobjekte weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Zu konfigurierende Richtlinie** des Assistenten auf **Erzeugung und Validierung von Eigenschaften**. Klicken Sie dann auf **Weiter**.

Klicken Sie auf der Seite **Kontrollierte Eigenschaft** auf **Auswählen**. Wählen Sie dann im Dialogfeld **Objekttyp und eigenschaft wählen** in der Liste **Objekttyp** den Eintrag **Benutzer** aus und klicken Sie in der Liste **Objekteigenschaft** auf **Rufnummer**, wie in der folgenden Abbildung gezeigt.

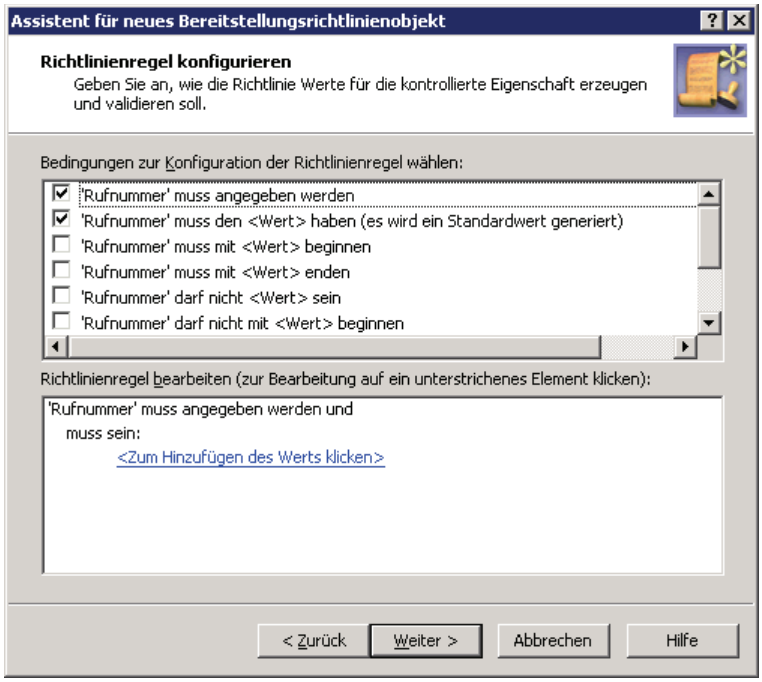


Klicken Sie auf **OK** und dann auf **Weiter**.

Aktivieren Sie auf der Seite **Richtlinienregel konfigurieren** im oberen Feld die folgenden Kontrollkästchen:

- **'Rufnummer' muss angegeben werden** (somit ist die Telefonnummer eine erforderliche Eigenschaft, es muss also in jedem Benutzerkonto eine Telefonnummer angegeben werden).
- **'Rufnummer' muss den <Wert>** haben (mit dieser Option können Sie eine Maske für die Telefonnummer konfigurieren, indem Sie dem Wert für diese Bedingung den entsprechenden Eintrag hinzufügen).

Nun entspricht die Seite **Richtlinienregeln konfigurieren** der folgenden Abbildung.



In der nächsten Phase wird der Wert konfiguriert.

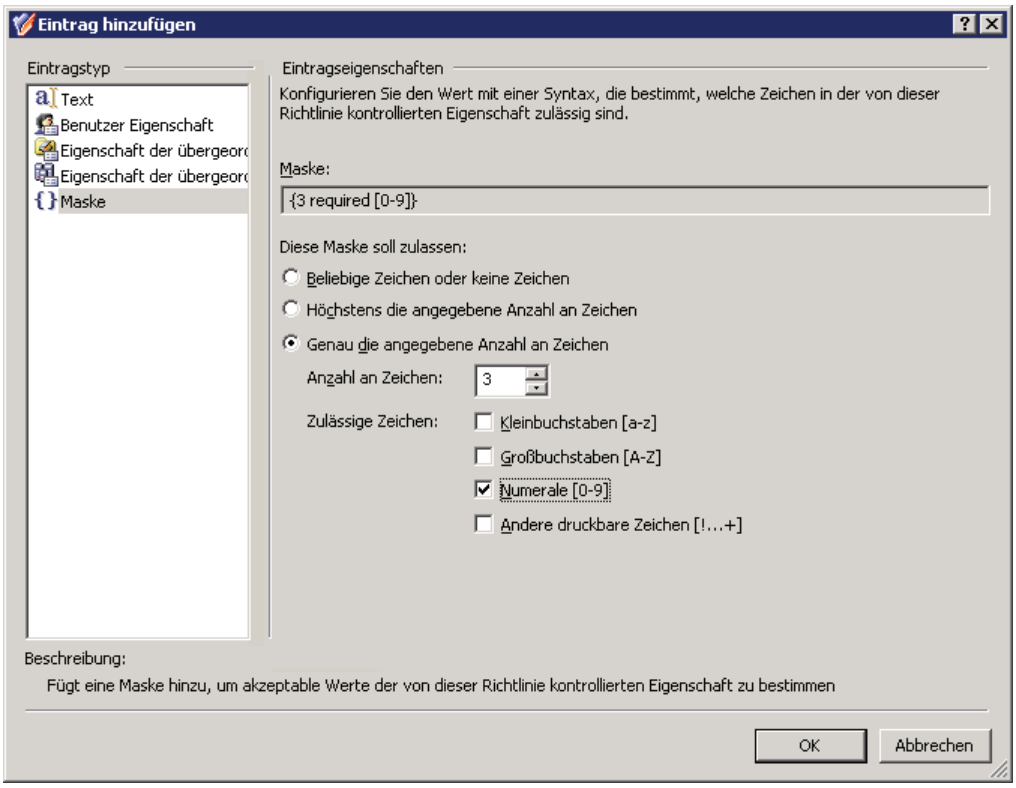
Klicken Sie auf die Verknüpfung mit der Beschriftung **<Zum Hinzufügen des Werts klicken>**. Klicken Sie im Dialogfeld **Wert hinzufügen** auf **Konfigurieren**. Klicken Sie im Dialogfeld **Wert konfigurieren** auf **Hinzufügen**. Klicken Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** auf **Maske**.

Jetzt können Sie im Fenster **Eintrag hinzufügen** im Bereich **Eintragseigenschaften** eine Maske konfigurieren.

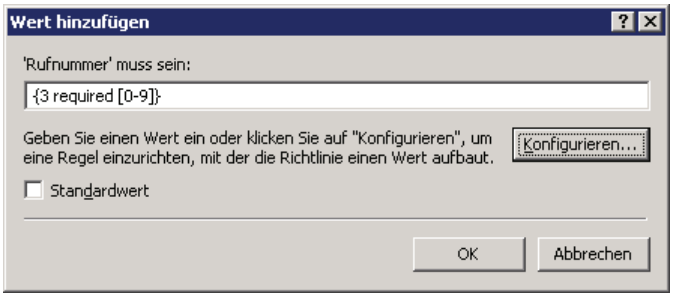
Das Format besteht aus vier Gruppen von Ziffern, die durch bestimmte Zeichen getrennt sind: Leerzeichen, Bindestriche und Klammern. Konfigurieren Sie zuerst eine Maske, die festlegt, dass die ersten drei Zeichen Ziffern sein müssen:

- Wählen Sie **Genau die angegebene Anzahl an Zeichen aus**.
- Geben Sie in das Feld **Anzahl an Zeichen** den Wert **3** ein.
- Aktivieren Sie unter **Zulässige Zeichen** das Kontrollkästchen **Numeral**.

Das Fenster **Eintrag hinzufügen** sollte nun der folgenden Abbildung entsprechen.



Klicken Sie auf **OK**, um das Fenster **Eintrag hinzufügen** zu schließen. Klicken Sie dann auf **OK**, um das Dialogfeld **Wert konfigurieren** zu schließen. Nunmehr sollte das Dialogfeld **Wert hinzufügen** der folgenden Abbildung entsprechen.

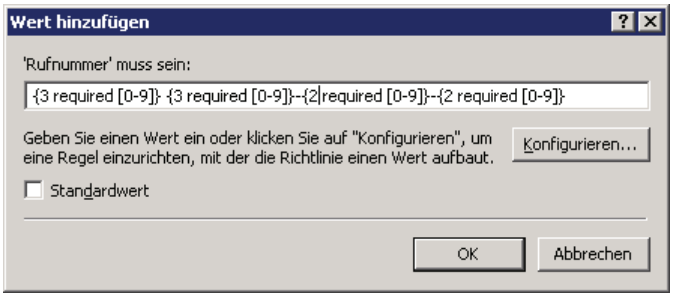

Wert hinzufügen
'Rufnummer' muss sein:
{3 required [0-9]}
Geben Sie einen Wert ein oder klicken Sie auf "Konfigurieren", um eine Regel einzurichten, mit der die Richtlinie einen Wert aufbaut.
Konfigurieren...
Standardwert
OK
Abbrechen

Sie können nun im Dialogfeld **Wert hinzufügen** die Maske bearbeiten.

Anhand der bereits konfigurierten Maske können Sie ahnen, dass Sie für das Telefonnummerformat folgende Maske benötigen:

```
({3 required [0-9]}) {3 required [0-9]}-{2 required [0-9]}-{2 required [0-9]}
```

Geben Sie diese Maske im Dialogfeld **Wert hinzufügen** in das Feld **'Rufnummer' muss sein** ein. Beachten Sie, dass die ersten drei Zeichen in runde Klammern eingeschlossen sind, dann ein Leerzeichen folgt, und dass zwei Bindestriche die Zeichengruppen trennen:


Wert hinzufügen
'Rufnummer' muss sein:
{3 required [0-9]} {3 required [0-9]}--{2|required [0-9]}--{2 required [0-9]}
Geben Sie einen Wert ein oder klicken Sie auf "Konfigurieren", um eine Regel einzurichten, mit der die Richtlinie einen Wert aufbaut.
Konfigurieren...
Standardwert
OK
Abbrechen

Klicken Sie auf **OK**, um das Dialogfeld **Wert hinzufügen** zu schließen. Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten für neues Bereitstellungsrichtlinienobjekt anwenden, oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen bezüglich der Anwendung eines Richtlinienobjekts finden Sie unter Anwenden von Richtlinienobjekten und Verwalten des Richtlinienbereichs weiter oben in diesem Kapitel.

Szenario 2: Durchsetzen eines Formats für Telefonnummern mit Hilfe regulärer Ausdrücke

In diesem Szenario wird beschrieben, wie Sie eine Richtlinie konfigurieren, die für die Telefonnummern von Benutzern das folgende Format durchsetzt:

- Das erste Zeichen muss „+" lauten
- Das bzw. die folgende(n) Zeichen müssen den Ländercode darstellen
- (Dieser lautet1 in den USA und in Kanada, und beispielsweise in Australien61)
- Die Vorwahl für die Stadt/Region muss mit Leerzeichen (und nicht mit Bindestrichen oder Klammern) abgetrennt sein
- Die Telefonnummer muss mit Leerzeichen (und nicht mit Bindestrichen) abgetrennt sein
- Optional kann die Durchwahl mit einem kleinen „x" angegeben werden

Die folgende Tabelle enthält Beispiele, die zeigen, wie die Telefonnummer anhand dieser Formatierungsanforderungen dargestellt werden muss.

RICHTIG	FALSCH	KOMMENTAR
+1 949 754 8515	949-754-8515	Der falsche Eintrag beginnt nicht mit „+" und dem Ländercode. Außerdem enthält er Bindestriche statt Leerzeichen.
+44 1628 606699 x1199	+44 1628 606699 x1199	Der falsche Eintrag enthält den Großbuchstaben X.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Folglich überprüft Quest One ActiveRoles beim Erstellen oder Ändern eines Benutzerobjekts in dem in Schritt 2 ausgewählten Container, ob die Telefonnummer dem angegebenen Format entspricht. Wenn sie ihm nicht entspricht, verbietet die Richtlinie die Erstellung oder Änderung des Benutzerobjekts.

Schritt 1: Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt konfigurieren, indem Sie das Richtlinienobjekt ändern, das das vorige Szenario implementiert; siehe „Szenario 1: Durchsetzen eines Formats für Telefonnummern mit Hilfe einer Maske" weiter oben in diesem Abschnitt.

Zeigen Sie das Dialogfeld **Eigenschaften** für dieses Richtlinienobjekt an und öffnen Sie die Registerkarte **Richtlinien**. Wählen Sie dann in der Liste die Richtlinie aus und klicken Sie auf **Anzeigen/Bearbeiten**, um das Dialogfeld **Eigenschaften der Eigenschaftsgenerierungs- und Validierungsrichtlinie** anzuzeigen.

Die Registerkarte **Richtlinienregel** im Dialogfeld **Eigenschaften der Eigenschaftsgenerierungs- und Validierungsrichtlinie** ähnelt der Seite **Richtlinienregel konfigurieren** des Assistenten, mit dem Sie die Richtlinie konfiguriert haben. Auf dieser Registerkarte können Sie die Richtlinienregeln ändern.

Ändern Sie die Regel zunächst, indem Sie den Maskeneintrag entfernen. Deaktivieren Sie auf der Registerkarte **Richtlinienregel** im oberen Feld das Kontrollkästchen **'Rufnummer' muss <Wert>** sein.

Wählen Sie dann aus, dass die Regel anhand regulärer Ausdrücke konfiguriert werden soll. Aktivieren Sie auf der Registerkarte **Richtlinienregel** im oberen Feld das Kontrollkästchen **'Rufnummer' muss regulärer Ausdruck <Wert>** sein. Um auf dieses Kontrollkästchen zuzugreifen, müssen Sie in der Liste der Kontrollkästchen einen Bildlauf nach unten ausführen.

Geben Sie zum Schluss die regulären Ausdrücke an, die die betreffende Richtlinie definieren. Sie benötigen folgende reguläre Ausdrücke:

```
^\+([0-9]+ )+[0-9]+$
^\+([0-9]+ )+x[0-9]+$
```

Die folgende Tabelle enthält eine kurze Beschreibung der Elemente, die in den beiden Syntaxzeichenfolgen oben verwendet werden. Weitere Informationen über reguläre Ausdrücke finden Sie in „Anhang A: Verwenden von regulären Ausdrücken" weiter unten in diesem Dokument.

ELEMENT	BEDEUTUNG
^	Der Anfang der zu überprüfenden Eingabezeichenfolge.
\+	Die Escapezeichenfolge zur Darstellung des Pluszeichens (+).
([0-9]+)+	Eine Verkettung von mindestens einer Teilzeichenfolge. Dabei besteht jede Teilzeichenfolge aus mindestens einer Ziffer, gefolgt von einem Leerzeichen.
[0-9]+	Mindestens eine Ziffer.
x[0-9]+	Der Kleinbuchstabe „x" gefolgt von mindestens einer Ziffer.
$	Das Ende der zu überprüfenden Eingabezeichenfolge.

Die Richtlinie muss also so konfiguriert werden, dass nur Telefonnummern zugelassen werden, die dem Ausdruck ^\+([0-9]+)+[0-9]+$ (ohne Durchwahl) oder ^\+([0-9]+)+x[0-9]+$ (mit Durchwahl) entsprechen. Konfigurieren Sie die Richtlinie desweiteren wie folgt:

1. Klicken Sie auf der Registerkarte **Richtlinienregel** im unteren Feld auf die Verknüpfung mit der Beschriftung **<Zum Hinzufügen des Werts klicken>**.
2. Geben Sie im Dialogfeld **Wert hinzufügen ^\+([0-9]+)+[0-9]+$** ein und klicken Sie dann auf **OK**.
3. Klicken Sie auf der Registerkarte **Richtlinienregel** im unteren Feld auf die Verknüpfung mit der Beschriftung **<Zum Hinzufügen des Werts klicken>**.
4. Geben Sie im Dialogfeld **Wert hinzufügen ^\+([0-9]+)+x[0-9]+$** ein und klicken Sie dann auf **OK**.
5. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften der Eigenschaftsgenerierungs- und Validierungsrichtlinie** zu schließen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt anwenden, ohne das zugehörige Dialogfeld **Eigenschaften** zu schließen. Rufen Sie die Registerkarte **Bereich** auf und gehen Sie folgendermaßen vor:

1. Klicken Sie auf der Registerkarte **Bereich** auf die Schaltfläche **Bereich**, um das Fenster **Quest One ActiveRoles-Richtlinienbereich** für das zu verwaltende Richtlinienobjekt anzuzeigen.
2. Klicken Sie auf **Hinzufügen** und wählen Sie die Domäne, Organisationseinheit oder verwaltete Einheit aus, auf die Sie die Richtlinie anwenden möchten.

   *Sie können auch mit Hilfe der Schaltfläche **Entfernen** Elemente entfernen, auf die die Richtlinie nicht mehr angewendet werden soll.*
3. Klicken Sie auf **OK**, um das Fenster **Quest One ActiveRoles-Richtlinienbereich** zu schließen.
4. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** für das Richtlinienobjekt zu schließen.

Weitere Informationen bezüglich der Anwendung eines Richtlinienobjekts finden Sie unter Anwenden von Richtlinienobjekten und Verwalten des Richtlinienbereichs weiter oben in diesem Kapitel.

Erzeugung von Benutzeranmeldenamen

Mit Richtlinien dieser Kategorie kann bei der Erstellung oder Änderung eines Benutzerkontos die Zuweisung des Benutzer-Anmeldenamens (Prä-Windows2000) automatisiert werden. Dabei stehen flexible Optionen zur Verfügung, um die Eindeutigkeit des von Richtlinien generierten Namens sicherzustellen.

Es ist sehr wichtig, dass ein eindeutiger Name generiert werden kann. Wenn Quest One ActiveRoles versucht, einen von einer Richtlinie generierten Namen zuzuweisen, wenn bereits ein Benutzerkonto mit demselben Benutzer-Anmeldenamen (Prä-Windows 2000) vorhanden ist, tritt ein Namenskonflikt auf. Active Directory unterstützt nicht mehrere Konten mit demselben Benutzer-Anmeldenamen (Prä Windows 2000). Eine Richtlinie kann so konfiguriert werden, dass sie eine Serie von Namen generiert, damit keine Namenskonflikte mit vorhandenen Konten auftreten.

Beim Konfigurieren einer Richtlinie dieser Kategorie können Sie mehrere Regeln definieren, die die Richtlinie bei einem Namenskonflikt nacheinander anwendet, um einen eindeutigen Namen zu generieren. Sie können auch eine Regel konfigurieren, mit der ein inkrementeller numerischer Wert eingeschlossen wird, um die Eindeutigkeit des von der Richtlinie konfigurierten Namens sicherzustellen. Außerdem besteht die Option, zuzulassen, dass Operatoren beim Erstellen oder Aktualisieren von Benutzerkonten die von Richtlinien konfigurierten Namen ändern.

Funktionsweise dieser Richtlinie

Beim Erstellen eines Benutzerkontos verwendet Quest One ActiveRoles diese Richtlinie, um dem Benutzerkonto einen bestimmten Namen von Versionen Prä-Windows 2000 zuzuweisen. Die Richtlinie generiert den Namen anhand der Eigenschaften des zu erstellenden Benutzerkontos. Eine Richtlinie kann mindestens eine Regel einschließen, die die Namenswerte als Verkettung von Einträgen konstruiert, die denen der Richtlinie „Erzeugung und Validierung von Eigenschaften" ähneln.

Ein besonderer Eintrag, die Eindeutigkeitszahl, wird bereitgestellt, um den von der Richtlinie generierten Namen eindeutig zu machen. Ein Eindeutigkeitszahleintrag stellt einen numerischen Wert dar, den die Richtlinie im Fall eines Namenskonflikts erhöht. Beispielsweise kann eine Richtlinie die Option bereitstellen, den neuen Namen von JSmith in J1Smith zu ändern, wenn bereits ein Benutzerkonto vorhanden ist, dessen Benutzer-Anmeldename (Prä-Windows 2000) auf JSmith festgelegt ist. Wenn auch der Name J1Smith bereits verwendet wird, kann der neue Name auf J2Smith geändert werden, und so weiter.

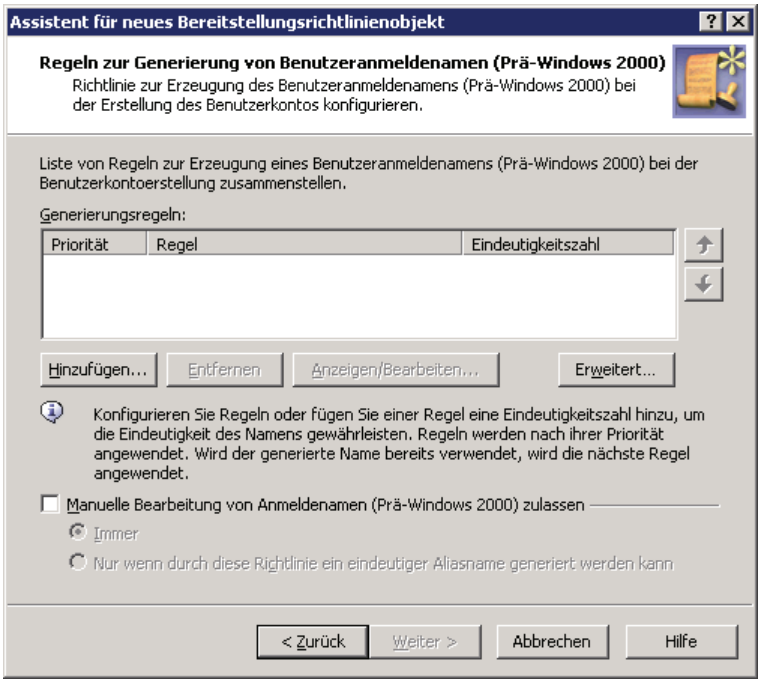
Bei der Richtlinienkonfiguration besteht die Option, die manuelle Bearbeitung von Namen, die durch Richtlinien generiert wurden, zuzulassen oder zu verweigern. Die Berechtigung zum Ändern eines Namens, der durch eine Richtlinie generiert wurde, kann auf den Fall eingeschränkt werden, dass der Name von einem anderen Konto verwendet wird.

Es folgen einige spezifische Aspekte des Richtlinienverhaltens:

- Mit einer einzelnen Regel, die keine Eindeutigkeitszahl verwendet, versucht Quest One ActiveRoles einfach, dem Benutzerkonto den generierten Namen zuzuweisen. Der Vorgang schlägt möglicherweise fehl, wenn der generierte Name nicht eindeutig ist, wenn also derselbe Benutzer-Anmeldename (Prä-Windows 2000) bereits einem anderen Benutzerkonto zugewiesen ist. Wenn die Richtlinie die manuelle Bearbeitung von Namen zulässt, die sie generiert hat, kann der Name von dem Operator korrigiert werden, der das Benutzerkonto erstellt.
- Wenn mehrere Regeln oder eine Regel mit Eindeutigkeitszahlen vorliegen, wird in Quest One ActiveRoles auf der Clientseite auf den Formularen für die Benutzererstellung und -änderung neben dem Feld **Benutzeranmeldename (Prä-Windows 2000)** eine Schaltfläche hinzugefügt.
- Um einen Namen zu generieren, muss der Clientbenutzer (Operator) auf diese Schaltfläche klicken, die auch die Situation abdeckt, in der der generierte Name bereits verwendet wird. Wenn Sie auf die Schaltfläche **Generieren** klicken, wird die nächste Regel angewendet, oder die Eindeutigkeitszahl wird um 1 erhöht, sodass ein eindeutiger Name vergeben werden kann.
- Die Richtlinie definiert eine Liste von Zeichen, die in Benutzer-Anmeldenamen (Prä-Windows 2000) nicht zulässig sind. Die folgenden Zeichen sind nicht zulässig: " / \ [ ] : ; | = , + * ? < >
- Die Richtlinie führt dazu, dass Quest One ActiveRoles die Verarbeitung von Vorgangsanforderungen ablehnt, die dem Benutzer-Anmeldenamen von Versionen Prä-Windows 2000 einen leeren Wert zuweisen würden.
- Bei der Überprüfung von Benutzerkonten auf die Richtlinieneinhaltung (siehe weiter unten in diesem Dokument) erkennt und berichtet Quest One ActiveRoles die Benutzer-Anmeldenamen (Prä-Windows 2000), die nicht so eingerichtet sind, wie die Richtlinie „Erzeugung von Benutzeranmeldenamen" vorschreibt.

Konfigurieren der Richtlinie „Erzeugung von Benutzeranmeldenamen“

Um die Richtlinie „Erzeugung von Benutzeranmeldenamen“ zu konfigurieren, wählen Sie **Erzeugung von Benutzeranmeldenamen** auf der Seite **Zu konfigurierende** Richtlinie im Assistenten für neues Bereitstellungsrichtlinienobjekt oder im Assistenten „Bereitstellungsrichtlinie hinzufügen“ aus. Klicken Sie dann auf **Weiter**, um die Seite **Regeln zur Generierung von Benutzeranmeldenamen (Prä Windows 2000)** anzuzeigen:


Assistent für neues Bereitstellungsrichtlinienobjekt
Regeln zur Generierung von Benutzeranmeldenamen (Prä-Windows 2000)
Richtlinie zur Erzeugung des Benutzeranmeldenamens (Prä-Windows 2000) bei der Erstellung des Benutzerkontos konfigurieren.
Liste von Regeln zur Erzeugung eines Benutzeranmeldenamens (Prä-Windows 2000) bei der Benutzerkontoerstellung zusammenstellen.
Generierungsregeln:
Priorität
Regel
Eindeutigkeitszahl
Hinzufügen...
Entfernen
Anzeigen/Bearbeiten...
Erweitert...
Konfigurieren Sie Regeln oder fügen Sie einer Regel eine Eindeutigkeitszahl hinzu, um die Eindeutigkeit des Namens gewährleisten. Regeln werden nach ihrer Priorität angewendet. Wird der generierte Name bereits verwendet, wird die nächste Regel angewendet.
Manuelle Bearbeitung von Anmeldenamen (Prä-Windows 2000) zulassen
Immer
Nur wenn durch diese Richtlinie ein eindeutiger Aliasname generiert werden kann
< Zurück
Weiter >
Abbrechen
Hilfe

Auf der Seite **Regeln zur Generierung von Benutzeranmeldenamen (Prä-Windows 2000)** können Sie eine Liste der Generierungsregeln aufstellen. Jeder Eintrag in der Liste schließt die folgenden Informationen ein:

- **Priorität.** Die Richtlinie wendet Generierungsregeln in der Reihenfolge ihrer Priorität an, die durch ihre Position in der Liste bestimmt wird: die zuerst gelesene Regel wird auch zuerst angewendet.
- **Regel.** Die Syntax, die die Regel definiert.
- **Eindeutigkeitszahl.** Zeigt **Ja** oder **Nein** an, um anzugeben, ob die Regel einen Eindeutigkeitszahleintrag enthält.

Sie können die Liste der Regeln mit folgenden Schaltflächen verwalten:

- **Hinzufügen.** Öffnet das Dialogfeld **Wert konfigurieren**, das weiter oben in diesem Kapitel beschrieben wurde (siehe „Konfigurieren einer Richtlinie für die Generierung und Validierung von Eigenschaften“). In diesem Dialogfeld können Sie einen Wert für die Bedingung **’Anmeldename (Prä-Windows 2000)’ muss sein** konfigurieren, ähnlich wie beim Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften“. Ausführlichere Informationen finden Sie unter „Konfigurieren einer Generierungsrichtlinie für Anmeldenamen“ weiter unten in diesem Abschnitt.
- **Entfernen.** Löscht die ausgewählten Regeln aus der Liste.

- **Anzeigen/Bearbeiten.** Öffnet das Dialogfeld **Wert konfigurieren** für die Regel, die Sie in der Liste auswählen. Sie können die ausgewählte Regel ändern, indem Sie die Liste der Einträge in diesem Dialogfeld verwalten.
- **Nach oben** und **Nach unten.** Ändert die Reihenfolge der Regeln in der Liste. Klicken Sie auf **Nach oben** oder **Nach unten**, um eine ausgewählte Regel in der Liste nach oben oder unten zu schieben, um also ihre Priorität zu erhöhen oder zu verringern.
- **Erweitert.** Legen Sie bestimmte Optionen fest, die auf alle Regeln in der Liste angewandt werden, wie etwa die maximale Länge des generierten Namens, ob der Name nur aus Großbuchstaben oder aus Groß- und Kleinbuchstaben formatiert werden soll, den Bereich, in dem der generierte Name eindeutig sein soll, und die Zeichen, die aus den generierten Namen ausgeschlossen werden sollen.

Durch Aktivieren des Kontrollkästchens **Manuelle Bearbeitung von Anmeldenamen (Prä Windows 2000) zulassen** autorisieren Sie den Operator, der das Benutzerkonto erstellt oder aktualisiert, zum Vornehmen von Änderungen an dem von der Richtlinie generierten Namen. Wenn dieses Kontrollkästchen deaktiviert ist, zeigt Quest One ActiveRoles in den Formularen zum Erstellen und Ändern von Benutzern das Feld **Benutzeranmeldename (Prä-Windows 2000)** schreibgeschützt an.

Durch Auswahl der Option **Immer** autorisieren Sie den Operator, den Prä-Windows 2000-Anmeldenamen nach Wunsch zu ändern. Mit der Option **Nur wenn durch diese Richtlinie ein eindeutiger Aliasname generiert werden kann** begrenzen Sie die manuellen Änderungen auf die Situation, in der kein eindeutiger Name in Übereinstimmung mit den Richtlinienregeln generiert werden kann.

Konfigurieren einer Generierungsrichtlinie für Anmeldenamen

Um eine Generierungsregel zu konfigurieren, klicken Sie unter der Liste **Generierungsregeln** auf die Schaltfläche **Hinzufügen**. Dann wird das Dialogfeld **Wert konfigurieren** angezeigt, in dem Sie aufgefordert werden, einen Wert für die Bedingung **'Anmeldename' muss sein** einzurichten.

Um mit dem Konfigurieren eines Wertes zu beginnen, klicken Sie im Dialogfeld **Hinzufügen** auf **Wert konfigurieren**. Daraufhin wird das Fenster **Eintrag hinzufügen** angezeigt:

Ein Wert entsteht durch Verkettung von mindestens einem Eintrag. Im Fenster **Eintrag hinzufügen** können Sie den Typ des hinzuzufügenden Eintrags auswählen und den Eintrag dann konfigurieren. In der folgenden Tabelle werden die verfügbaren Eintragstypen zusammengefasst.

EINTRAGSTYP	BESCHREIBUNG
Text	Fügt dem Wert eine Textzeichenfolge hinzu.
Eindeutigkeitszahl	Fügt einen numerischen Wert hinzu, den die Richtlinie bei einem Namenskonflikt erhöhen soll.
Benutzereigenschaft	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) des Benutzerkontos hinzu, dem die Richtlinie den Anmeldenamen zuweist.
Eigenschaft der übergeordneten Organisationseinheit	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) einer Organisationseinheit in der Containerhierarchie über dem Benutzerkonto hinzu, dem die Richtlinie den Anmeldenamen zuweist.
Eigenschaft der übergeordneten Domäne	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) der Domäne des Benutzerkontos hinzu, dem die Richtlinie den Anmeldenamen zuweist.

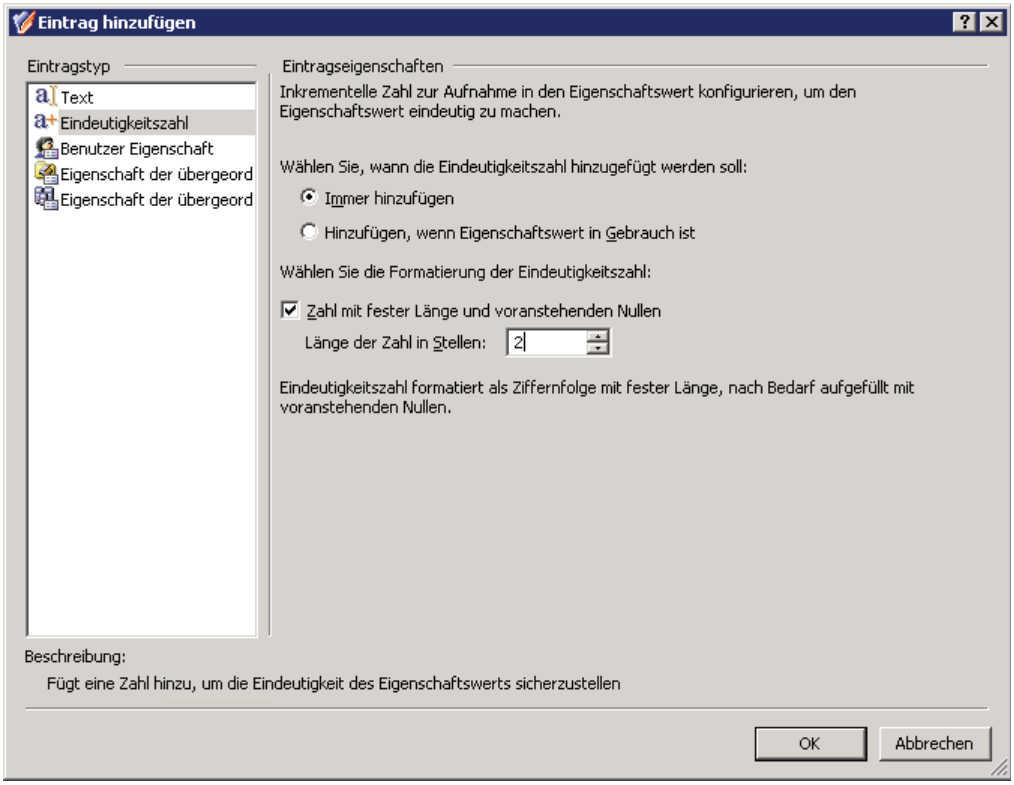
Die Anweisungen zum Konfigurieren eines Eintrags hängen vom Eintragstyp ab. Sie können die im Abschnitt Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften“ weiter oben in diesem Kapitel beschriebenen Anweisungen befolgen, um einen Eintrag eines der folgenden Typen zu konfigurieren:

- **Text.** Siehe Unterabschnitt Eintragstyp: Text.
- **Benutzereigenschaft.** Siehe Unterabschnitt Eintragstyp: <Objekt>eigenschaft.
- **Eigenschaft der übergeordneten Organisationseinheit.** Siehe Unterabschnitt Eintragstyp: Eigenschaft der übergeordneten Organisationseinheit.
- **Eigenschaft der übergeordneten Domäne.** Siehe Unterabschnitt Eintragstyp: Eigenschaft der übergeordneten Domäne.

Im folgenden Unterabschnitt wird der Eintrag **Eindeutigkeitszahl** erörtert.

Eintragstyp: Eindeutigkeitszahl

Wenn Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** den Typ **Eindeutigkeitszahl** auswählen, ähnelt der Bereich **Eintragseigenschaften** der folgenden Abbildung.


Eintrag hinzufügen
Eintragstyp
Text
Eindeutigkeitszahl
Benutzer Eigenschaft
Eigenschaft der übergeord
Eigenschaft der übergeord
Eintragseigenschaften
Inkrementelle Zahl zur Aufnahme in den Eigenschaftswert konfigurieren, um den Eigenschaftswert eindeutig zu machen.
Wählen Sie, wann die Eindeutigkeitszahl hinzugefügt werden soll:
Immer hinzufügen
Hinzufügen, wenn Eigenschaftswert in Gebrauch ist
Wählen Sie die Formatierung der Eindeutigkeitszahl:
Zahl mit fester Länge und voranstehenden Nullen
Länge der Zahl in Stellen:
2
Eindeutigkeitszahl formatiert als Ziffernfolge mit fester Länge, nach Bedarf aufgefüllt mit voranstehenden Nullen.
Beschreibung:
Fügt eine Zahl hinzu, um die Eindeutigkeit des Eigenschaftswerts sicherzustellen
OK
Abbrechen

Mit diesem Eintragstyp können Sie einen Eintrag hinzufügen, der eine Zahl darstellt, den die Richtlinie im Fall eines Namenskonflikts erhöht.

Sie müssen zuerst auswählen, wann die Richtlinie diesen Eintrag verwenden soll. Folgende Optionen stehen zur Verfügung:

- **Immer hinzufügen.** Der Wert schließt diesen Eintrag unabhängig davon ein, ob die Richtlinie bei der Anwendung der Generierungsregel einen Namenskonflikt erkennt.
- **Hinzufügen, wenn Eigenschaftswert in Gebrauch ist.** Die Richtlinie fügt diesen Eintrag bei einem Namenskonflikt zum Wert hinzu; ansonsten enthält dieser Wert nicht diesen Eintrag.

Als Nächstes können Sie angeben, wie der Eintrag formatiert werden soll:

- Damit er als Ziffernfolge variabler Länge formatiert wird, deaktivieren Sie das Kontrollkästchen **Zahl mit fester Länge und voranstehenden Nullen**. In den meisten Fällen ergibt dies einen Eintrag aus nur einer Ziffer.
- Damit der Eintrag als Ziffernfolge fester Länge formatiert wird, aktivieren Sie das Kontrollkästchen **Zahl mit fester Länge und voranstehenden Nullen** und geben Sie dann die gewünschte Ziffernanzahl ein. Dies generiert einen Eintrag mit der passenden Anzahl von Nullen als Präfix, z.B. 001, 002, 003.

Klicken Sie nach dem Konfigurieren eines Eintrags auf **OK**, um das Fenster **Eintrag hinzufügen** zu schließen. Der Eintrag wird dem Dialogfeld **Wert konfigurieren** hinzugefügt.

Verfahren zum Konfigurieren einer Richtlinie bezüglich der Generierung eines Benutzeranmeldenamens

So konfigurieren Sie eine Richtlinie für die Generierung von Benutzer-Anmeldenamen:

1. Wählen Sie auf der Seite **Zu konfigurierende Richtlinie** die Option **Erzeugung von Benutzeranmeldenamen** aus und klicken Sie dann auf **Weiter**.
2. Gehen Sie auf der Seite **Regeln zur Generierung von Benutzeranmeldenamen (Prä Windows 2000)** wie nachfolgend beschrieben vor und klicken Sie dann auf **Weiter**:
   - Klicken Sie auf **Hinzufügen** und vervollständigen Sie das Dialogfeld **Wert konfigurieren**, indem Sie das weiter unten in diesem Thema beschriebene Verfahren befolgen, um eine Namensgenerierungsregel zu erstellen.
   - Wählen Sie eine Regel aus und klicken Sie dann auf **Entfernen**, um die Regel zu löschen.
   - Wählen Sie eine Regel aus und klicken Sie dann auf **Anzeigen/Bearbeiten**, um die Regel zu ändern.
   - Wählen Sie eine Regel aus und klicken Sie dann auf **Nach oben** oder **Nach unten**, um die Regel in der Liste nach oben oder unten zu verschieben, um somit ihre Priorität zu erhöhen bzw. zu verringern.
   - Klicken Sie auf **Erweitert**, um einige Optionen festzulegen, die für alle Regeln innerhalb der Richtlinie gelten. Schließen Sie das Dialogfeld **Erweitert** ab, indem Sie das weiter unten in diesem Thema beschriebene Verfahren befolgen.
   - Wenn Sie die manuelle Bearbeitung des Anmeldenamens ermöglichen möchten, wählen Sie die Option **Manuelle Bearbeitung von Anmeldenamen (Prä-Windows 2000) zulassen** aus. Führen Sie dann eine der folgenden Aktionen durch:
     - Klicken Sie auf **Immer**, um dem Operator, der das Benutzerkonto erstellt oder aktualisiert, die Änderung des Prä-Windows 2000-Anmeldenamens zu ermöglichen.
     - Klicken Sie auf **Nur wenn durch diese Richtlinie ein eindeutiger Aliasname generiert werden kann**, wenn Sie manuelle Änderungen auf den Fall beschränken möchten, dass ein richtliniengenerierter Name bereits einem anderen Benutzerkonto zugewiesen ist.

3. Auf der Seite **Richtlinie erzwingen** können Sie Objekte angeben, auf die dieses Richtlinienobjekt angewandt werden soll:
   - Klicken Sie auf **Hinzufügen** und verwenden Sie das Objekt **Objekte auswählen**, um die gewünschten Objekte auszuwählen.
4. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Gehen Sie folgendermaßen vor, um das Dialogfeld „Wert konfigurieren" abzuschließen:

1. Klicken Sie auf **Hinzufügen**.
2. Konfigurieren Sie einen Eintrag, in den der Wert aufgenommen werden soll (Anweisungen finden Sie unter Verfahren zum Konfigurieren von Einträgen).
3. Im Dialogfeld **Wert konfigurieren** fügen Sie Einträge hinzu, löschen oder bearbeiten vorhandene Einträge und klicken dann auf **OK**.

Gehen Sie folgendermaßen vor, um das Dialogfeld „Erweitert" abzuschließen:

1. Legen Sie unter **Maximale Länge in Zeichen** die maximale Länge des generierten Namens fest.
2. Aktivieren Sie optional **Groß-/Kleinschreibung der Zeichen anpassen**, um die Groß/Kleinschreibung zu konfigurieren:
   - Klicken Sie auf **Alle GROSS**, um den Namen als eine aus Großbuchstaben bestehende Zeichenkette zu formatieren.
   - Klicken Sie auf **Alle klein**, um den Namen als eine aus Kleinbuchstaben bestehende Zeichenkette zu formatieren.
3. Geben Sie den Bereich ein, in dem der generierte Name eindeutig sein soll.
   - Klicken Sie auf **Domäne**, wenn der Name innerhalb der Domäne eindeutig sein soll.
   - Klicken Sie auf **Gesamtstruktur**, wenn der Name innerhalb der Gesamtstruktur eindeutig sein soll.
   - Klicken Sie auf **Allen verwalteten Domänen**, um den Namen eindeutig für alle verwalteten Domänen festzulegen.
4. Geben Sie optional im Bereich **Beschränkte Zeichen** die Zeichen an, die die Richtlinie aus dem generierten Namen entfernen soll.

   Die Richtlinie entfernt immer die folgenden Zeichen: "@+|=\:;?[],<>/ Um weitere Zeichen anzugeben, geben Sie diese nacheinander ohne jegliches Trennzeichen in dem zu diesem Zweck vorgesehenen Textfeld ein.*

Szenario 1: Verwenden einer Eindeutigkeitszahl

Die in diesem Szenario beschriebene Richtlinie generiert den Benutzer-Anmeldenamen (Prä-Windows 2000) in Übereinstimmung mit folgender Regel: das erste Zeichen des Vornamens des Benutzers, dann optional eine Eindeutigkeitszahl, dann der Nachname des Benutzers. Der von der Richtlinie generierte Name ist höchstens 8 Zeichen lang. Wenn der Name länger ist, werden die hinteren Zeichen bei Bedarf abgeschnitten. Es folgen Beispiele für Namen, die von dieser Richtlinie generiert werden:

- JSmitson
- J1Smitso
- J2Smitso

Die Richtlinie generiert den Namen J1Smitso für den Benutzer John Smitson, falls der Name JSmitson bereits verwendet wird. Wenn JSmitson und J1Smitso schon verwendet werden, generiert die Richtlinie den Namen J2Smitso usw.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Wenn Sie nun einem Benutzerkonto in dem in Schritt 2 ausgewählten Container einen Benutzer-Anmeldenamen (Prä-Windows 2000) zuweisen, stellen die Benutzeroberflächen von Quest One ActiveRoles die Schaltfläche **Generieren** bereit, mit der ein Name in Übereinstimmung mit der Richtlinienregel erstellt werden kann. Wenn Sie im Fall eines Namenskonflikts auf die Schaltfläche **Generieren** klicken, fügt die Richtlinie dem Namen eine Eindeutigkeitszahl hinzu.

In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten für neues Bereitstellungsrichtlinienobjekt erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter Erstellen eines Richtlinienobjekts im Abschnitt Verwaltungsaufgaben für Richtlinienobjekte weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Richtlinientyp auswählen** des Assistenten auf **Erzeugung von Benutzeranmeldenamen**. Klicken Sie dann auf **Weiter**.

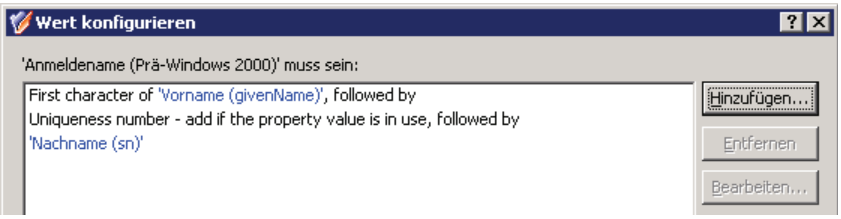
Klicken Sie auf der Seite **Regeln zur Generierung von Benutzeranmeldenamen (Prä-Windows 2000)** auf **Hinzufügen**. Füllen Sie dann das Dialogfeld **Wert konfigurieren** wie folgt aus:

1. Klicken Sie auf **Hinzufügen**.
2. Konfigurieren Sie den Eintrag so, dass das erste Zeichen des Vornamens des Benutzers eingeschlossen wird:
   a) Klicken Sie unter **Eintragstyp** auf **Benutzereigenschaft**.
   b) Klicken Sie unter **Eintragseigenschaften** auf **Auswählen**.
   c) Klicken Sie im Fenster **Objekteigenschaft wählen** auf **Vorname** in der Liste **Objekteigenschaft** und klicken Sie dann auf **OK**.
   d) Klicken Sie unter **Eintragseigenschaften** auf **Die ersten**, und stellen Sie sicher, dass das Feld neben dieser Option den Wert **1** enthält.
   e) Klicken Sie auf **OK**.
3. Klicken Sie auf **Hinzufügen**.
4. Konfigurieren Sie wie folgt den Eintrag so, dass er optional eine Eindeutigkeitszahl enthält:
   a) Klicken Sie unter **Eintragstyp** auf **Eindeutigkeitszahl**.
   b) Klicken Sie unter **Eintragseigenschaften** auf **Hinzufügen, wenn Eigenschaftswert in Gebrauch ist**, und stellen Sie sicher, dass das Kontrollkästchen **Zahl mit fester Länge und voranstehenden Nullen** deaktiviert ist.
   c) Klicken Sie auf **OK**.
5. Klicken Sie auf **Hinzufügen**.
6. Konfigurieren Sie den Eintrag so, dass er den Nachnamen des Benutzers enthält:
   a) Klicken Sie unter **Eintragstyp** auf **Benutzereigenschaft**.
   b) Klicken Sie unter **Eintragseigenschaften** auf **Auswählen**.

c) Klicken Sie im Fenster **Objekteigenschaft wählen** auf **Nachname** in der Liste **Objekteigenschaft** und klicken Sie dann auf **OK**.

d) Klicken Sie auf **OK**.

Nach dem Ausführen dieser Schritte sollte die Liste der Einträge im Dialogfeld **Wert konfigurieren** der folgenden Abbildung ähneln.


Wert konfigurieren
'Anmeldename (Prä-Windows 2000)' muss sein:
First character of 'Vorname (givenName)', followed by
Uniqueness number - add if the property value is in use, followed by
'Nachname (sn)'
Hinzufügen...
Entfernen
Bearbeiten...

Klicken Sie auf **OK**, um das **Dialogfeld Wert** konfigurieren zu schließen.

Richten Sie nun die Grenze für die Namenslänge ein. Klicken Sie auf der Seite **Regeln zur Generierung von Benutzeranmeldenamen (Prä-Windows 2000)** auf die Schaltfläche **Erweitert**. Geben Sie im Dialogfeld **Erweitert** im Feld **Maximale Länge in Zeichen 8** ein und klicken Sie dann auf **OK**.

Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten für neues Bereitstellungsrichtlinienobjekt anwenden, oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen bezüglich der Anwendung eines Richtlinienobjekts finden Sie unter Anwenden von Richtlinienobjekten und Verwalten des Richtlinienbereichs weiter oben in diesem Kapitel.

Szenario 2: Verwenden mehrerer Regeln

Die in diesem Szenario beschriebene Richtlinie verwendet mehrere Regeln, um den Benutzer-Anmeldenamen (Prä-Windows 2000) zu generieren. Die Regeln lauten wie folgt:

1. Das erste Zeichen des Vornamens des Benutzers, gefolgt vom Nachnamen des Benutzers.
2. Die ersten beiden Zeichen des Vornamens des Benutzers, gefolgt vom Nachnamen des Benutzers.
3. Die ersten drei Zeichen des Vornamens des Benutzers, gefolgt vom Nachnamen des Benutzers.

Der von der Richtlinie generierte Name ist höchstens 8 Zeichen lang. Wenn der Name länger ist, werden die hinteren Zeichen bei Bedarf abgeschnitten.

Es folgen Beispiele für Namen, die von dieser Richtlinie generiert werden:

- JSmitson
- JoSmitso
- JohSmits

Die Richtlinie generiert den Namen JoSmitso für den Benutzer John Smitson, falls der Name JSmitson bereits verwendet wird. Wenn JSmitson und JoSmitso schon verwendet werden, generiert die Richtlinie den Namen JohSmits.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Wenn Sie nun einem Benutzerkonto in dem in Schritt 2 ausgewählten Container einen Benutzer-Anmeldenamen (Prä-Windows 2000) zuweisen, stellen die Benutzeroberflächen von Quest One ActiveRoles die Schaltfläche **Generieren** bereit, mit der der Name in Übereinstimmung mit den Richtlinienregeln erstellt werden kann. Wenn Sie im Fall eines Namenskonflikts auf die Schaltfläche **Generieren** klicken, verwendet die Richtlinie eine der folgenden Regeln.

In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

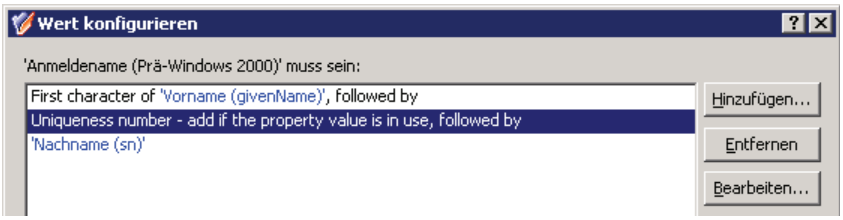
Schritt 1: Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt konfigurieren, indem Sie das Richtlinienobjekt ändern, das das vorige Szenario implementiert; siehe „Szenario 1: Verwenden einer Eindeutigkeitszahl" weiter oben in diesem Abschnitt.

Zeigen Sie das Dialogfeld **Eigenschaften** für dieses Richtlinienobjekt an und öffnen Sie die Registerkarte **Richtlinien**. Wählen Sie dann in der Liste die Richtlinie aus und klicken Sie auf **Anzeigen/Bearbeiten**, um das Dialogfeld **Eigenschaften der Benutzeranmeldenamen-Generierungsrichtlinie** anzuzeigen.

Die Registerkarte **Generierungsregeln** im Dialogfeld **Eigenschaften der Benutzeranmeldenamen-Generierungsrichtlinie** ähnelt der Seite **Regeln zur Generierung von Benutzeranmeldenamen (Prä-Windows 2000)** des Assistenten, mit dem Sie die Richtlinie konfiguriert haben. Auf dieser Registerkarte können Sie Richtlinienregeln hinzufügen oder ändern.

Ändern Sie die Regel zunächst, indem Sie den Eintrag für die Eindeutigkeitszahl entfernen. Wählen Sie auf der Registerkarte **Generierungsregeln** die Regel aus und klicken Sie auf **Anzeigen/Bearbeiten**, um das Dialogfeld **Wert konfigurieren** anzuzeigen. Wählen Sie dann den Eindeutigkeitszahleintrag aus, wie in der folgenden Abbildung gezeigt, und klicken Sie auf **Entfernen**.

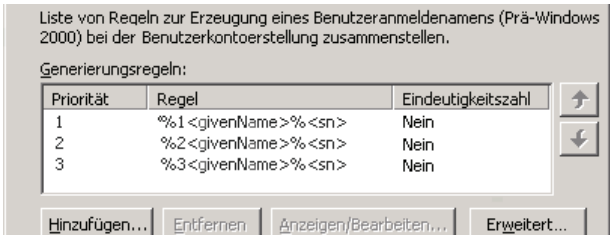

Wert konfigurieren
'Anmeldename (Prä-Windows 2000)' muss sein:
First character of 'Vorname (givenName)', followed by
Uniqueness number - add if the property value is in use, followed by
'Nachname (sn)'
Hinzufügen...
Entfernen
Bearbeiten...

Klicken Sie auf **OK**, um das **Dialogfeld Wert** konfigurieren zu schließen.

Konfigurieren Sie nun wie folgt die zusätzlichen Richtlinienregeln:

1. Klicken Sie auf der Registerkarte **Generierungsregeln** auf **Hinzufügen**, um das Dialogfeld **Wert konfigurieren** anzuzeigen.
2. Klicken Sie im Dialogfeld **Wert konfigurieren** auf **Hinzufügen**, um das Fenster **Eintrag hinzufügen** anzuzeigen.
3. Konfigurieren Sie den Eintrag so, dass die ersten beiden Zeichen des Vornamens des Benutzers eingeschlossen wird:
   a) Klicken Sie unter **Eintragstyp** auf **Benutzereigenschaft**.
   b) Klicken Sie unter **Eintragseigenschaften** auf **Auswählen**.
   c) Klicken Sie im Fenster **Objekteigenschaft wählen** auf **Vorname** in der Liste **Objekteigenschaft** und klicken Sie dann auf **OK**.
   d) Klicken Sie unter **Eintragseigenschaften** auf **Die ersten** und geben Sie in das Feld neben dieser Option den Wert **2** ein.
   e) Klicken Sie auf **OK**, um das Fenster **Eintrag hinzufügen** zu schließen.
4. Klicken Sie im Dialogfeld **Wert konfigurieren** auf **Hinzufügen**, um das Fenster **Eintrag hinzufügen** anzuzeigen.
5. Konfigurieren Sie den Eintrag so, dass er den Nachnamen des Benutzers enthält:
   a) Klicken Sie unter **Eintragstyp** auf **Benutzereigenschaft**.
   b) Klicken Sie unter **Eintragseigenschaften** auf **Auswählen**.
   c) Klicken Sie im Fenster **Objekteigenschaft wählen** auf **Nachname** in der Liste **Objekteigenschaft** und klicken Sie dann auf **OK**.
   d) Klicken Sie auf **OK**, um das Fenster **Eintrag hinzufügen** zu schließen.
6. Klicken Sie auf **OK**, um das **Dialogfeld Wert** konfigurieren zu schließen.
7. Wiederholen Sie die Schritte 1 bis 6 mit folgender Abweichung:
   Geben Sie in Schritt 3 im Teilschritt d) in das Feld neben der Option **Die ersten** den Wert **3** ein.

Nach der Ausführung dieser Schritte sollte die Liste der Regeln auf der Registerkarte **Generierungsregeln** folgendes Aussehen aufweisen:



Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften der Benutzeranmeldenamen-Generierungsrichtlinie** zu schließen.

Schritt 2: Anwenden des Richtlinienobjekts

Um das Richtlinienobjekt anzuwenden, können Sie im Dialogfeld **Eigenschaften** für dieses Richtlinienobjekt die Registerkarte **Bereich** verwenden:

1. Klicken Sie auf der Registerkarte **Bereich** auf die Schaltfläche **Bereich**, um das Fenster **Quest One ActiveRoles-Richtlinienbereich** für das zu verwaltende Richtlinienobjekt anzuzeigen.
2. Klicken Sie auf **Hinzufügen** und wählen Sie die Domäne, Organisationseinheit oder verwaltete Einheit aus, auf die Sie die Richtlinie anwenden möchten.

   *Sie können auch mit Hilfe der Schaltfläche **Entfernen** Elemente entfernen, auf die die Richtlinie nicht mehr angewendet werden soll.*
3. Klicken Sie auf **OK**, um das Fenster **Quest One ActiveRoles-Richtlinienbereich** zu schließen.
4. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** für das Richtlinienobjekt zu schließen.

Weitere Informationen bezüglich der Anwendung eines Richtlinienobjekts finden Sie unter Anwenden von Richtlinienobjekten und Verwalten des Richtlinienbereichs weiter oben in diesem Kapitel.

Automatische Bereitstellung der Gruppenmitgliedschaft

Richtlinien dieser Kategorie dienen zum Automatisieren des Hinzufügens oder Entfernens angegebener Objekte wie z.B. Benutzerobjekte in angegebenen Gruppen.

Sie können Objekttypen sowie Gruppen auswählen und Richtlinienregeln einrichten. Die Richtlinie fügt den ausgewählten Gruppen Objekte hinzu oder entfernt sie daraus, je nachdem, ob diese Objekte den angegebenen Regeln entsprechen.

Funktionsweise dieser Richtlinie

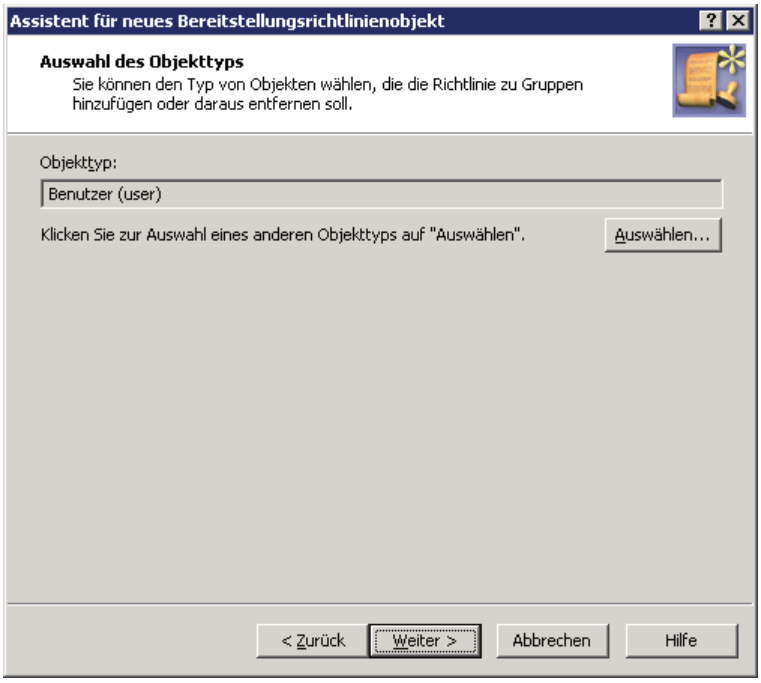
Die Richtlinie „Automatische Bereitstellung der Gruppenmitgliedschaft" für die Gruppenmitgliedschaft führt Bereitstellungsaufgaben aus, wie das Hinzufügen oder Entfernen von Benutzern in Gruppen. Eine Richtlinie kann so konfiguriert werden, dass sie eine Liste von Gruppen und Bedingungen definiert, wobei den Gruppen ein Benutzerkonto automatisch hinzugefügt bzw. aus ihnen entfernt wird, je nachdem, ob die Eigenschaften des Benutzerkontos die Richtlinienbedingungen erfüllen.

Quest One ActiveRoles überprüft Benutzer automatisch anhand von Bedingungen und fügt die Benutzer basierend auf den Überprüfungsergebnissen angegebenen Gruppen hinzu oder entfernt sie aus diesen. Zwar ähneln die Funktionen dieser Richtlinie denen dynamischer Gruppen; die Richtlinie „Automatische Bereitstellung der Gruppenmitgliedschaft" ermöglicht dem Administrator jedoch zusätzliche Flexibilität und Kontrolle über Gruppenmitgliedschaften.

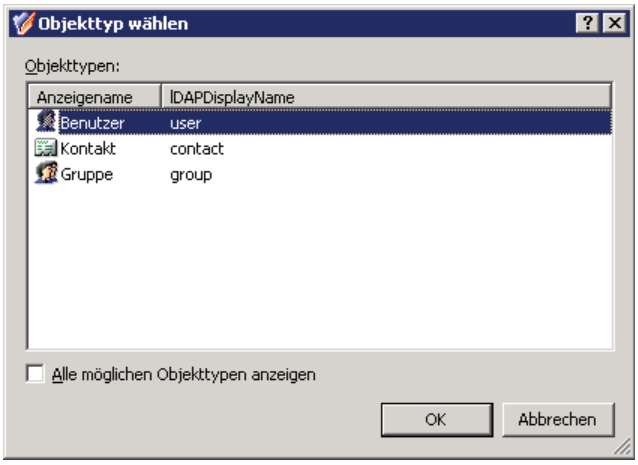
Während die Funktion für dynamische Gruppen einen regelorientierten Verwaltungsmechanismus für die Verwaltung der gesamten Gruppenmitgliedschaftsliste bietet, ermöglicht die Richtlinie „Automatische Bereitstellung der Gruppenmitgliedschaft" dem Administrator das Definieren von Mitgliedschaftsregeln für einzelne Benutzer. Diese Richtlinie automatisiert das Hinzufügen bestimmter Benutzer zu bestimmten Gruppen ohne Auswirkungen auf die anderen Mitglieder dieser Gruppen.

Konfigurieren der Richtlinie „Automatische Bereitstellung der Gruppenmitgliedschaft“

Um die Richtlinie „Automatische Bereitstellung der Gruppenmitgliedschaft“ zu konfigurieren, wählen Sie **Automatische Bereitstellung der Gruppenmitgliedschaft** auf der Seite **Zu konfigurierende** Richtlinie im Assistenten für neues Bereitstellungsrichtlinienobjekt oder im Assistenten „Bereitstellungsrichtlinie hinzufügen“ aus. Klicken Sie dann auf **Weiter**, damit die Seite **Auswahl des Objekttyps** angezeigt wird.

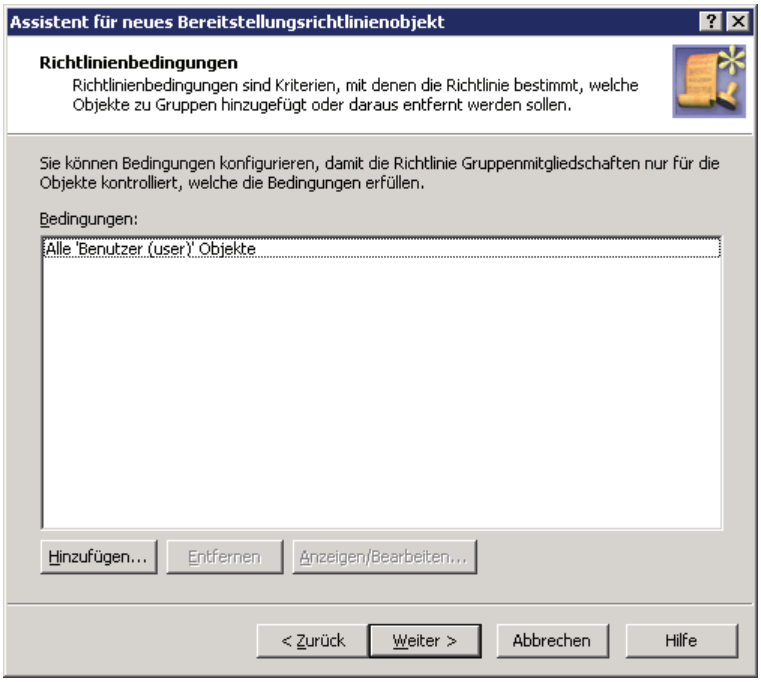

Assistent für neues Bereitstellungsrichtlinienobjekt
Auswahl des Objekttyps
Sie können den Typ von Objekten wählen, die die Richtlinie zu Gruppen hinzufügen oder daraus entfernen soll.
Objekttyp:
Benutzer (user)
Klicken Sie zur Auswahl eines anderen Objekttyps auf "Auswählen".
Auswählen...
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite können Sie den Typ von Objekten auswählen, die die Richtlinie zu Gruppen hinzufügen oder aus ihnen entfernen soll. Standardmäßig ist der Objekttyp auf „Benutzer“ festgelegt. Wenn Sie diese Einstellung ändern möchten, klicken Sie auf **Auswählen**, um das Dialogfeld **Objekttyp wählen** anzuzeigen.



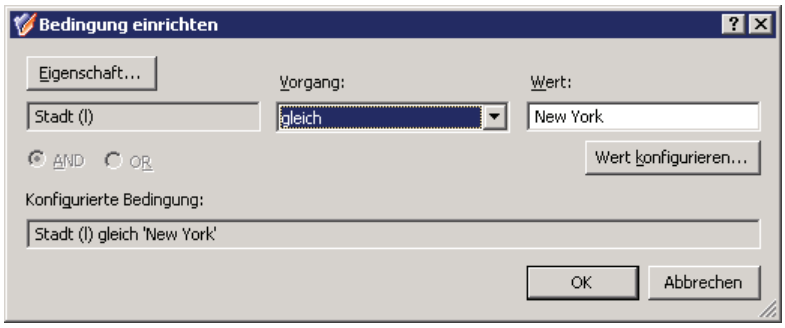
Wählen Sie in der Liste **Objekttypen** den Typ der Objekte aus, die die Richtlinie steuern soll. Klicken Sie auf **OK**.

Klicken Sie auf der Seite **Auswahl des Objekttyps** auf **Weiter**, um die Seite **Richtlinienbedingungen** anzuzeigen.


Assistent für neues Bereitstellungsrichtlinienobjekt
Richtlinienbedingungen
Richtlinienbedingungen sind Kriterien, mit denen die Richtlinie bestimmt, welche Objekte zu Gruppen hinzugefügt oder daraus entfernt werden sollen.
Sie können Bedingungen konfigurieren, damit die Richtlinie Gruppenmitgliedschaften nur für die Objekte kontrolliert, welche die Bedingungen erfüllen.
Bedingungen:
Alle 'Benutzer (user)' Objekte
Hinzufügen...
Entfernen
Anzeigen/Bearbeiten...
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite können Sie Richtlinienbedingungen einrichten, also Kriterien, mit denen die Richtlinie bestimmt, welche Objekte zu Gruppen hinzugefügt bzw. aus ihnen entfernt werden. Wenn Sie keine Bedingungen angeben, wirkt sich die Richtlinie auf alle Objekte des auf der vorigen Seite ausgewählten Typs aus. Wenn Sie auf dieser Seite Bedingungen angeben, wirkt sie sich nur auf die Objekte aus, die sie erfüllen.

Klicken Sie zum Konfigurieren einer Bedingung auf der Seite **Richtlinienbedingungen** auf **Hinzufügen**. Nun wird das Dialogfeld **Bedingung einrichten** angezeigt.



In diesem Dialogfeld können Sie eine Bedingung auf die gleiche Weise konfigurieren wie für eine Richtlinie „Erzeugung und Validierung von Eigenschaften". Eine Bedingung enthält eine Objekteigenschaft (beispielsweise **Stadt** oder **Abteilung**), eine Anforderung (beispielsweise **gleich** oder **beginnt mit**) und einen Wert. Der Begriff *Wert* hat dieselbe Bedeutung wie für die Richtlinie „Erzeugung und Validierung von Eigenschaften".

Klicken Sie zuerst auf die Schaltfläche **Eigenschaft**, um das Dialogfeld **Objekteigenschaft wählen** anzuzeigen, in dem Sie die Objekteigenschaft auswählen können, die in die Bedingung eingeschlossen werden soll.

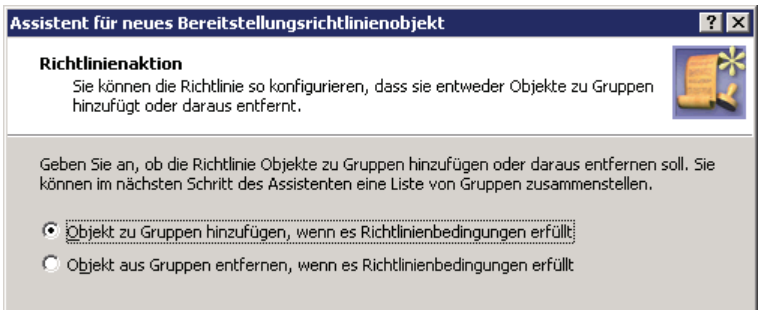
Wählen Sie dann in der Liste **Vorgang** die Anforderung aus, die Sie auf die ausgewählte Eigenschaft anwenden möchten.

Klicken Sie nun auf die Schaltfläche **Wert konfigurieren**, um den Wert einzurichten, auf den Sie die ausgewählte Anforderung anwenden möchten. Hierdurch wird das Dialogfeld **Wert konfigurieren** geöffnet, das weiter oben in diesem Kapitel beschrieben wurde (siehe „Konfigurieren einer Richtlinie für die Generierung und Validierung von Eigenschaften"). In diesem Dialogfeld können Sie einen Wert auf die gleiche Weise einrichten wie für die Richtlinie „Erzeugung und Validierung von Eigenschaften".

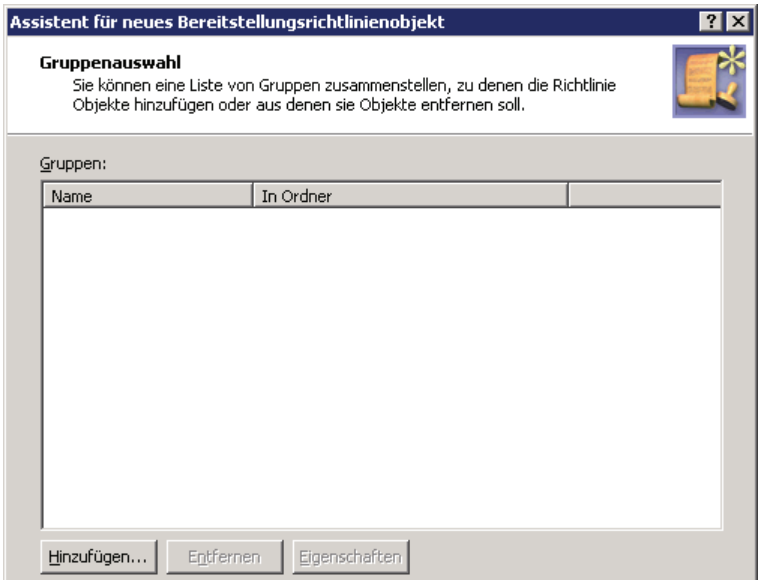
Wenn Sie mehrere Bedingungen angeben, können Sie diese durch Klicken auf **UND** bzw. **ODER** mit einem logischen „und" – oder „oder"-Operator verknüpfen.

Klicken Sie abschließend auf **OK**, um das Dialogfeld **Bedingung einrichten** zu schließen.

Wenn Sie die Liste auf der Seite **Richtlinienbedingungen** fertig gestellt haben, klicken Sie auf **Weiter**, um die Seite **Richtlinienaktion** anzuzeigen:


Assistent für neues Bereitstellungsrichtlinienobjekt
Richtlinienaktion
Sie können die Richtlinie so konfigurieren, dass sie entweder Objekte zu Gruppen hinzufügt oder daraus entfernt.
Geben Sie an, ob die Richtlinie Objekte zu Gruppen hinzufügen oder daraus entfernen soll. Sie können im nächsten Schritt des Assistenten eine Liste von Gruppen zusammenstellen.
Objekt zu Gruppen hinzufügen, wenn es Richtlinienbedingungen erfüllt
Objekt aus Gruppen entfernen, wenn es Richtlinienbedingungen erfüllt

Auf dieser Seite können Sie die Richtlinie so konfigurieren, dass Sie Objekte zu Gruppen hinzufügt oder aus ihnen entfernt. Wenn Sie beispielsweise die Option **Objekt zu Gruppen hinzufügen, wenn es Richtlinienbedingungen erfüllt** auswählen, füllt die Richtlinie Gruppen mit den Objekten auf, die die im vorigen Schritt eingerichteten Bedingungen erfüllen. Klicken Sie auf **Weiter**, um die Gruppen anzugeben, die die Richtlinie auffüllen soll. Hierdurch wird die Seite **Gruppenauswahl** angezeigt.



Auf der Seite **Gruppenauswahl** können Sie eine Liste von Gruppen einrichten, die von der Richtlinie gesteuert werden sollen. Abhängig von der im vorigen Schritt ausgewählten Option fügt die Richtlinie jeder auf dieser Seite angegebenen Gruppe Objekte hinzu oder entfernt Objekte aus ihr. Sie können die Liste mit Hilfe der Schaltflächen **Hinzufügen** und **Entfernen** verwalten. Durch Anklicken von **Hinzufügen** wird das Dialogfeld O**bjekte auswählen** angezeigt, in dem Sie Gruppe auswählen und zur Liste hinzufügen können. Wenn Sie auf **Entfernen** klicken, werden die ausgewählten Einträge aus der Liste gelöscht.

Klicken Sie nach dem Einrichten der Gruppenliste auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Verfahren zum Konfigurieren der Richtlinie „Automatische Bereitstellung der Gruppenmitgliedschaft"

So konfigurieren Sie eine Richtlinie zur automatische Bereitstellung von Gruppenmitgliedschaften:

1. Wählen Sie auf der Seite **Zu konfigurierende Richtlinie** die Option **Automatische Bereitstellung der Gruppenmitgliedschaft** aus und klicken Sie dann auf **Weiter**.
2. Klicken Sie auf **Wählen**, um den Typ des Objekts anzugeben, das die Richtlinie zu den Gruppen hinzufügen oder aus den Gruppen entfernen soll. Schließen Sie das Dialogfeld **Objekttyp wählen** ab, indem Sie das weiter unten in diesem Thema beschriebene Verfahren befolgen. Klicken Sie dann auf **Weiter**.
3. Konfigurieren Sie auf der Seite **Richtlinienbedingungen** Bedingungen, die festlegen, wie die Richtlinie zu Gruppen hinzuzufügende Objekte oder aus Gruppen zu entfernende Objekte auswählt, und klicken Sie dann auf **Weiter**:
   - Klicken Sie zur Erstellung einer neuen Bedingung auf **Hinzufügen**. Schließen Sie das Dialogfeld **Bedingung einrichten** ab, indem Sie das weiter unten in diesem Thema beschriebene Verfahren befolgen.

- Wählen Sie eine Bedingung aus und klicken Sie dann auf **Entfernen**, um die Bedingung zu löschen.
- Wählen Sie eine Bedingung aus und klicken Sie dann auf **Anzeigen/Bearbeiten**, um die Bedingung zu ändern.

4. Geben Sie auf der Seite **Richtlinienvorgang** an, ob die Richtlinie Objekte zu Gruppen hinzufügen oder aus diesen entfernen soll, indem Sie die entsprechende Option aktivieren, und klicken Sie dann auf **Weiter**.
5. Konfigurieren Sie auf der Seite **Gruppenauswahl** eine Liste der Gruppen, zu der die Richtlinie Objekte hinzuzufügen oder aus der die Richtlinie Objekte entfernen soll:
   - Klicken Sie auf **Hinzufügen** und verwenden Sie das Dialogfeld **Objekte auswählen**, um die gewünschten Gruppen auszuwählen.
6. Auf der Seite **Richtlinie erzwingen** können Sie Objekte angeben, auf die dieses Richtlinienobjekt angewandt werden soll:
   - Klicken Sie auf **Hinzufügen** und verwenden Sie das Objekt **Objekte auswählen**, um die gewünschten Objekte auszuwählen.
7. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Gehen Sie folgendermaßen vor, um das Dialogfeld „Objekttyp auswählen" abzuschließen:

- Wählen Sie in der Liste **Objekttypen** den Typ des Objekts aus, das die Richtlinie zu Gruppen hinzufügen oder aus Gruppen entfernen soll und klicken Sie dann auf **OK**.

*Wenn der benötigte Objekttyp nicht angezeigt wird, wählen Sie **Alle möglichen Objekttypen anzeigen**.*

Gehen Sie folgendermaßen vor, um das Dialogfeld „Bedingung konfigurieren" abzuschließen:

1. Klicken Sie auf **Eigenschaft**, um die Eigenschaft auszuwählen, für die Sie die Bedingung konfigurieren möchten.
2. Klicken Sie unter **Objekteigenschaft** auf die gewünschte Eigenschaft. Klicken Sie dann auf **OK**.

   *Wenn die benötigte Eigenschaft nicht angezeigt wird, wählen Sie **Alle mögliche Eigenschaften anzeigen**.*
3. Klicken Sie unter **Vorgang** auf den Vorgang für die Bedingung.
4. Geben Sie unter **Wert** eine Variable ein, um die Bedingung zu präzisieren. Klicken Sie dann auf **OK**.

   – ODER –

   Klicken Sie auf **Wert konfigurieren** und folgen den nächsten Schritten.
5. Klicken Sie auf **Hinzufügen**.
6. Konfigurieren Sie im Dialogfeld **Eintrag hinzufügen** einen Eintrag (Anweisungen finden Sie unter Verfahren zum Konfigurieren von Einträgen) und klicken Sie dann auf **OK**.
7. Im Dialogfeld **Wert konfigurieren** fügen Sie Einträge hinzu, löschen oder bearbeiten vorhandene Einträge und klicken dann auf **OK**.

Szenario: Hinzufügen von Benutzern zu einer angegebenen Gruppe

Die in diesem Szenario beschriebene Richtlinie fügt automatisch Benutzerkonten den angegebenen Gruppen hinzu, in Abhängigkeit von der Eigenschaft der **Department** Benutzerkonten. Wenn die Eigenschaft **Department** eines Benutzerkontos auf **Vertrieb** festgelegt ist, fügt die Richtlinie das Konto der Gruppe **Vertrieb** hinzu.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie ein Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Wenn für ein Benutzerkonto in dem in Schritt 2 ausgewählten Container die Eigenschaft **Department** auf **Vertrieb** festgelegt ist, fügt Quest One ActiveRoles das Konto folglich automatisch der Gruppe **Vertrieb** hinzu.

In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten für neues Bereitstellungsrichtlinienobjekt erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter Erstellen eines Richtlinienobjekts im Abschnitt Verwaltungsaufgaben für Richtlinienobjekte weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Richtlinientyp auswählen** des Assistenten auf **Automatische Bereitstellung der Gruppenmitgliedschaft**. Klicken Sie dann auf **Weiter**.

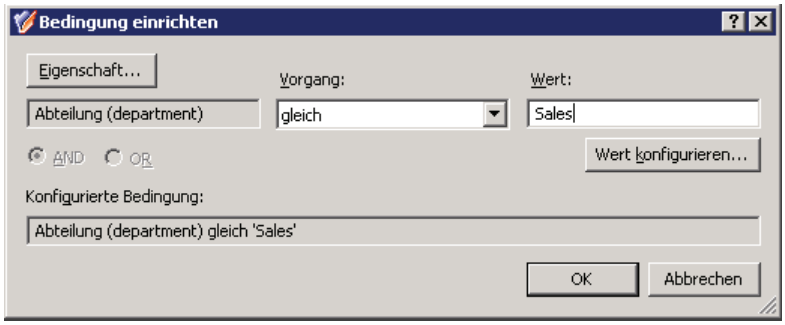
Klicken Sie auf der Seite **Auswahl des Objekttyps** auf **Weiter**, um die Standardeinstellung zu akzeptieren, also den Objekttyp für Benutzer.

Klicken Sie auf der Seite **Richtlinienbedingungen** auf **Hinzufügen**, um das Dialogfeld **Bedingung einrichten** anzuzeigen.

Konfigurieren Sie die Bedingung wie folgt:

1. Klicken Sie auf die Schaltfläche **Eigenschaft**. Aktivieren Sie dann das Kontrollkästchen **Abteilung** und klicken Sie anschließend auf **OK**.
2. Geben Sie in das Feld **Wert** den Wert **Vertrieb** ein.

Nach der Ausführung dieser Schritte entspricht das Dialogfeld **Bedingung einrichten** der folgenden Abbildung.



Klicken Sie auf **OK**, um das Dialogfeld **Bedingung einrichten** zu schließen.

Klicken Sie auf der Seite **Richtlinienbedingungen** auf **Weiter**.

Klicken Sie auf der Seite **Richtlinienaktion** auf **Objekt zu Gruppen hinzufügen, wenn es Richtlinienbedingungen erfüllt** und klicken Sie dann auf **Weiter**.

Klicken Sie auf der Seite **Gruppenauswahl** auf **Hinzufügen** und suchen Sie dann im Dialogfeld **Objekte auswählen** die Gruppe **Vertrieb**. Wenn Sie die Gruppe **Vertrieb** zu der Liste auf der Seite **Gruppenauswahl** hinzugefügt haben, klicken Sie auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten für neues Bereitstellungsrichtlinienobjekt anwenden, oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen bezüglich der Anwendung eines Richtlinienobjekts finden Sie unter Anwenden von Richtlinienobjekten und Verwalten des Richtlinienbereichs weiter oben in diesem Kapitel.

E-Mail-Aliaserzeugung

Richtlinien dieser Kategorie dienen zum Automatisieren der Zuweisung des E-Mail-Alias, wenn ein Benutzer in Microsoft Exchange Server für die Verwendung von Postfächern aktiviert wird. Standardmäßig stellt Microsoft Exchange Server das folgende Format für E-Mail-Adressen von Empfängern bereit: *<E-Mail-Alias>*@*<Domänenname>*

Sie können E-Mail-Aliase mittels vordefinierter Regeln generieren oder benutzerdefinierte Regeln konfigurieren. Sie können beispielsweise eine Richtlinie konfigurieren, mit der der E-Mail-Alias aus dem Anfangsbuchstaben des Vornamens und dem Nachnamen des Benutzers zusammengestellt wird. Mit Hilfe benutzerdefinierter Regeln können Sie einen inkrementellen numerischen Wert hinzufügen, um die Eindeutigkeit des Alias sicherzustellen. Sie können auch angeben, ob der Alias von dem Operator geändert werden kann, der das Benutzerkonto erstellt oder aktualisiert.

Funktionsweise dieser Richtlinie

Wenn ein Benutzer für die Verwendung von Postfächern aktiviert wird, verwendet Quest One ActiveRoles diese Richtlinie, um dem Benutzerkonto einen bestimmten E-Mail-Alias zuzuweisen. Die Richtlinie generiert den Alias basierend auf Benutzereigenschaften, z.B. dem Benutzer-Anmeldenamen (Prä Windows 2000), dem Vornamen, den Initialen und dem Nachnamen. Zum Verwenden anderer Eigenschaften kann eine benutzerdefinierte Regel konfiguriert werden.

Außerdem kann eine benutzerdefinierte Regel konfiguriert werden, um eine so genannte *Eindeutigkeitszahl* hinzuzufügen. Die Eindeutigkeitszahl ist ein numerischer Wert, den die Richtlinie in den Alias einschließt und den sie bei einem Aliasnamenskonflikt erhöht. Die Richtlinie kann beispielsweise automatisch den generierten Alias von John.Smith in John1.Smith ändern, wenn bereits ein Postfach mit dem Alias John.Smith vorhanden ist. Wenn auch der Alias John1.Smith bereits verwendet wird, wird der neue Alias in John2.Smith geändert und so weiter.

Bei der Richtlinienkonfiguration besteht die Option, die manuelle Bearbeitung von Aliasen, die durch Richtlinien generiert wurden, zuzulassen oder zu verweigern. Die Berechtigung zum Ändern eines Alias, der durch eine Richtlinie generiert wurde, kann auf den Fall eingeschränkt werden, dass der Alias von einem anderen Postfach verwendet wird.

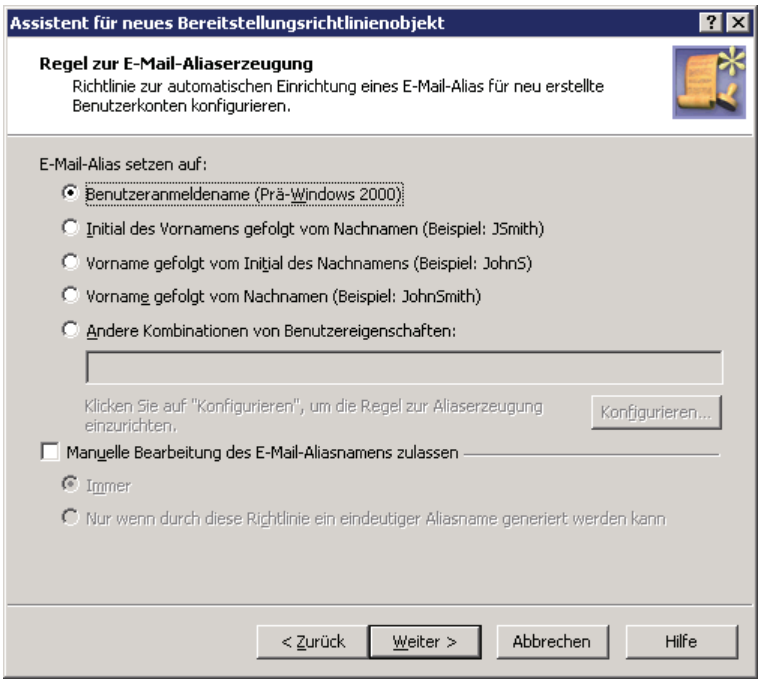
Es folgen einige spezifische Aspekte des Richtlinienverhaltens:

- Mit einer Regel, die keine Eindeutigkeitszahl verwendet, versucht Quest One ActiveRoles einfach, dem Benutzerkonto den generierten Alias zuzuweisen. Dieser Vorgang kann fehlschlagen, wenn der generierte Alias nicht eindeutig ist, wenn er also schon einem anderen Benutzerkonto zugewiesen wurde. Wenn die Richtlinie die manuelle Bearbeitung von Aliasen zulässt, die sie generiert hat, kann der Alias von dem Operator korrigiert werden, der das Benutzerkonto erstellt.
- Wenn eine benutzerdefinierte Regel mit Eindeutigkeitszahlen vorliegen, wird in Quest One ActiveRoles auf der Clientseite auf den Formularen für die Benutzererstellung und -änderung neben dem Feld **Alias** eine Schaltfläche hinzugefügt.

  Um einen Alias zu generieren, muss der Clientbenutzer (Operator) auf diese Schaltfläche klicken, die auch die Situation abdeckt, in der der generierte Alias bereits verwendet wird. Durch Klicken auf die Schaltfläche **Generieren** wird die Eindeutigkeitszahl um1 erhöht und ermöglicht so einen eindeutigen Alias.
- Wenn eine benutzerdefinierte Regel konfiguriert wurde, um Benutzereigenschaften einzuschließen, die normalerweise in den Benutzererstellungsformularen nicht angezeigt werden, wird auf der Quest One ActiveRoles-Konsole dem Assistenten „Neues Objekt – Benutzer" eine zusätzliche Seite hinzugefügt. Somit können die für die Aliasgenerierung erforderlichen Eigenschaften angegeben werden.
- Die Richtlinie definiert eine Liste von Zeichen, die in Benutzer-Anmeldenamen E-Mail-Aliase. Zulässig sind weder Leerzeichen noch die folgenden Zeichen: @ * + | = \ ; : ? [ ] , < > /
- Die Richtlinie führt dazu, dass Quest One ActiveRoles die Verarbeitung von Vorgangsanforderungen ablehnt, die dem E-Mail-Alias einen leeren Wert zuweisen würden.
- Bei der Überprüfung von Benutzerkonten auf die Richtlinieneinhaltung (siehe weiter unten in diesem Dokument) erkennt und berichtet Quest One ActiveRoles die Aliase, die nicht so eingerichtet sind, wie die Generierungsrichtlinie für Aliase vorschreibt.

Konfigurieren der Richtlinie „E-Mail-Aliaserzeugung“

Um die Richtlinie **„E-Mail-Aliaserzeugung“** zu konfigurieren, wählen Sie E-Mail-Aliaserzeugung auf der Seite **Zu konfigurierende Richtlinie** im Assistenten für neues Bereitstellungsrichtlinienobjekt oder im Assistenten „Bereitstellungsrichtlinie hinzufügen“ aus. Klicken Sie dann auf **Weiter**, um die Seite Regel zur **E-Mail-Aliaserzeugung** anzuzeigen:


Assistent für neues Bereitstellungsrichtlinienobjekt
Regel zur E-Mail-Aliaserzeugung
Richtlinie zur automatischen Einrichtung eines E-Mail-Alias für neu erstellte Benutzerkonten konfigurieren.
E-Mail-Alias setzen auf:
Benutzeranmeldename (Prä-Windows 2000)
Initial des Vornamens gefolgt vom Nachnamen (Beispiel: JSmith)
Vorname gefolgt vom Initial des Nachnamens (Beispiel: JohnS)
Vorname gefolgt vom Nachnamen (Beispiel: JohnSmith)
Andere Kombinationen von Benutzereigenschaften:
Klicken Sie auf "Konfigurieren", um die Regel zur Aliaserzeugung einzurichten.
Konfigurieren...
Manuelle Bearbeitung des E-Mail-Aliasnamens zulassen
Immer
Nur wenn durch diese Richtlinie ein eindeutiger Aliasname generiert werden kann
< Zurück
Weiter >
Abbrechen
Hilfe

Auf der Seite **Regel zur E-Mail-Aliaserzeugung** können Sie eine vorkonfigurierte Regel auswählen oder eine benutzerdefinierte Richtlinie zur E-Mail-Aliasgenerierung erstellen. Die ersten vier Optionen auf der Seite sind selbsterklärend. Beispielsweise erstellt die erste Option einen E-Mail-Alias, der dem Benutzer-Anmeldenamen (Prä-Windows 2000) entspricht. Die Option **Andere Kombinationen von Benutzereigenschaften**, die weiter unten in diesem Abschnitt erörtert wird, ermöglicht das Konfigurieren einer benutzerdefinierten Regel, der auch eine Eindeutigkeitszahl hinzugefügt werden kann.

Durch Aktivieren des Kontrollkästchens **Manuelle Bearbeitung des E-Mail-Aliasnamens zulassen** autorisieren Sie den Operator, der das Benutzerkonto erstellt oder aktualisiert, zum Vornehmen von Änderungen an dem von der Richtlinie generierten Alias. Wenn dieses Kontrollkästchen deaktiviert ist, zeigt Quest One ActiveRoles in den Formularen zum Erstellen und Ändern von Benutzern das Feld **Alias** schreibgeschützt an.

Indem Sie die Option **Immer** auswählen, autorisieren Sie den Operator, den Alias nach Wunsch zu ändern. Mit der Option **Nur wenn durch diese Richtlinie ein eindeutiger Aliasname generiert werden kann** begrenzen Sie die manuellen Änderungen auf die Situation, in der kein eindeutiger Alias in Übereinstimmung mit den Richtlinienregeln generiert werden kann.

Konfigurieren einer benutzerdefinierten Richtlinie zur E-Mail-Aliasgenerierung

Um eine benutzerdefinierte Regel zu konfigurieren, klicken Sie auf **Andere Kombinationen von Benutzereigenschaften** und dann auf die Schaltfläche **Konfigurieren**. Hierdurch wird das Dialogfeld **Wert konfigurieren** geöffnet, das weiter oben in diesem Kapitel beschrieben wurde (siehe „Konfigurieren einer Richtlinie für die Generierung und Validierung von Eigenschaften"). In diesem Dialogfeld können Sie einen Wert für die Bedingung **'Alias' muss sein** konfigurieren, ähnlich wie beim Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften".

Um mit dem Konfigurieren eines Wertes zu beginnen, klicken Sie im Dialogfeld **Hinzufügen** auf **Wert konfigurieren**. Daraufhin wird das Fenster **Eintrag hinzufügen** angezeigt:

Ein Wert entsteht durch Verkettung von mindestens einem Eintrag. Im Fenster **Eintrag hinzufügen** können Sie den Typ des hinzuzufügenden Eintrags auswählen und den Eintrag dann konfigurieren. In der folgenden Tabelle werden die verfügbaren Eintragstypen zusammengefasst.

EINTRAGSTYP	BESCHREIBUNG
Text	Fügt dem Wert eine Textzeichenfolge hinzu.
Eindeutigkeitszahl	Fügt einen numerischen Wert hinzu, den die Richtlinie bei einem Aliasnamenskonflikt erhöhen soll.
Benutzereigenschaft	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) des Benutzerkontos hinzu, dem die Richtlinie den Alias zuweist.
Eigenschaft der übergeordneten Organisationseinheit	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) einer Organisationseinheit in der Containerhierarchie über dem Benutzerkonto hinzu, dem die Richtlinie den Alias zuweist.
Eigenschaft der übergeordneten Domäne	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) der Domäne des Benutzerkontos hinzu, dem die Richtlinie den Alias zuweist.

Die Anweisungen zum Konfigurieren eines Eintrags hängen vom Eintragstyp ab. Sie finden Anweisungen für jeden Eintragstyp weiter oben in diesem Kapitel:

- **Text.** Weitere Informationen finden Sie im Unterabschnitt Eintragstyp: Text im Abschnitt Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften".
- **Eindeutigkeitszahl.** Weitere Informationen finden Sie im Unterabschnitt Eintragstyp: Eindeutigkeitszahl im Abschnitt Konfigurieren der Richtlinie „Erzeugung von Benutzeranmeldenamen".
- **Benutzereigenschaft.** Weitere Informationen finden Sie im Unterabschnitt Eintragstyp: <Objekt>eigenschaft im Abschnitt Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften".
- **Eigenschaft der übergeordneten Organisationseinheit.** Weitere Informationen finden Sie im Unterabschnitt Eintragstyp: Eigenschaft der übergeordneten Organisationseinheit im Abschnitt Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften".
- **Eigenschaft der übergeordneten Domäne.** Weitere Informationen finden Sie im Unterabschnitt Eintragstyp: Eigenschaft der übergeordneten Domäne im Abschnitt Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften".

Klicken Sie nach dem Konfigurieren eines Wertes auf **OK**, um das Dialogfeld **Wert konfigurieren** zu schließen. Damit wird der Wert zur Eigenschaftsrichtlinie hinzugefügt. Nötigenfalls können Sie den Wert ändern. Klicken Sie dazu auf die Schaltfläche **Konfigurieren** und verwalten Sie dann die Liste der Einträge im Dialogfeld **Wert konfigurieren**.

Klicken Sie nach dem Konfigurieren der Richtlinienregeln auf **Weiter** auf der Seite **Regel zur E-Mail-Aliaserzeugung** und befolgen Sie die Anweisungen im Assistenten, um das Richtlinienobjekt zu erstellen.

Verfahren zum Konfigurieren der Richtlinie „E-Mail-Aliaserzeugung"

So konfigurieren Sie eine Richtlinie „E-Mail-Aliaserzeugung":

1. Wählen Sie auf der Seite **Zu konfigurierende Richtlinie** die Option **E-Mail-Aliaserzeugung** aus und klicken Sie dann auf **Weiter**.
2. Gehen Sie auf der Seite **E-Mail-Alias-Generierungsregel** wie nachfolgend beschrieben vor und klicken Sie dann auf **Weiter**.
   - Wählen Sie eine der vorkonfigurierten Generierungsregeln aus oder erstellen Sie eine benutzerdefinierte Alias-Generierungsregel. Um eine benutzerdefinierte Regel zu erstellen, klicken Sie auf **Andere Kombinationen von Benutzereigenschaften**, klicken Sie dann auf **Konfigurieren** und schließen Sie das Dialogfeld **Wert konfigurieren** ab, indem Sie das weiter unten in diesem Thema beschriebene Verfahren befolgen.
   - Wenn Sie die manuelle Bearbeitung des E-Mail-Alias ermöglichen möchten, wählen Sie die Option **Manuelle Bearbeitung des E-Mail-Aliasnamens zulassen** aus. Führen Sie anschließend eine der folgenden Aktionen durch:
     - Klicken Sie auf **Immer**, um dem Operator, der das Benutzerkonto erstellt oder aktualisiert, die Änderung des E-Mail-Alias zu ermöglichen.
     - Klicken Sie auf **Nur wenn durch diese Richtlinie ein eindeutiger Aliasname generiert werden kann**, wenn Sie manuelle Änderungen auf den Fall beschränken möchten, dass ein richtliniengenerierter Aliasname bereits einem anderen Benutzerkonto zugewiesen ist.
3. Auf der Seite **Richtlinie erzwingen** können Sie Objekte angeben, auf die dieses Richtlinienobjekt angewandt werden soll:
   - Klicken Sie auf **Hinzufügen** und verwenden Sie das Objekt **Objekte auswählen**, um die gewünschten Objekte auszuwählen.
4. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Gehen Sie folgendermaßen vor, um das Dialogfeld „Wert konfigurieren" abzuschließen:

1. Klicken Sie auf **Hinzufügen**.
2. Konfigurieren Sie einen Eintrag, in den der Wert aufgenommen werden soll (Anweisungen finden Sie unter Verfahren zum Konfigurieren von Einträgen).
3. Im Dialogfeld **Wert konfigurieren** fügen Sie Einträge hinzu, löschen oder bearbeiten vorhandene Einträge und klicken dann auf **OK**.

Szenario: Generieren von E-Mail-Aliasen anhand von Benutzernamen

Die in diesem Szenario beschriebene Richtlinie generiert den E-Mail-Alias anhand der folgenden Regel: Vorname des Benutzers, optional eine dreistellige Eindeutigkeitszahl, dann ein Punkt und dann der Nachname des Benutzers. Es folgen Beispiele für Aliase, die von dieser Regel generiert werden:

- John.Smith
- John001.Smith
- John002.Smith

Die Richtlinie generiert den Alias John001.Smith für den Benutzer John Smith, falls der Alias John.Smith bereits verwendet wird. Wenn John.Smith und John001.Smith schon verwendet werden, generiert die Richtlinie den Alias John002.Smith, usw.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Wenn Sie nun einem Benutzerkonto in dem in Schritt 2 ausgewählten Container einen E-Mail-Alias zuweisen, stellen die Benutzeroberflächen von Quest One ActiveRoles die Schaltfläche **Generieren** bereit, mit der der Alias in Übereinstimmung mit der Richtlinienregel erstellt werden kann. Wenn Sie im Fall eines Aliasnamenskonflikts auf die Schaltfläche **Generieren** klicken, fügt die Richtlinie dem Alias eine Eindeutigkeitszahl hinzu.

In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten für neues Bereitstellungsrichtlinienobjekt erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter Erstellen eines Richtlinienobjekts im Abschnitt Verwaltungsaufgaben für Richtlinienobjekte weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Richtlinientyp auswählen** des Assistenten auf **E-Mail-Aliaserzeugung**. Klicken Sie dann auf **Weiter**.

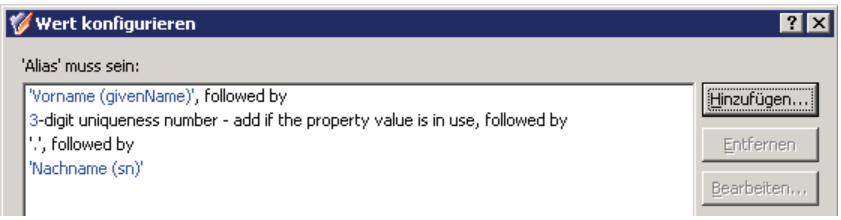
Klicken Sie auf der Seite **Regel zur E-Mail-Aliaserzeugung** auf **Andere Kombinationen von Benutzereigenschaften** und klicken Sie dann auf **Konfigurieren**.

Füllen Sie das Dialogfeld **Wert konfigurieren** wie folgt aus:

1. Klicken Sie auf **Hinzufügen**.
2. Konfigurieren Sie den Eintrag so, dass er den Vornamen des Benutzers enthält:
   a) Klicken Sie unter **Eintragstyp** auf **Benutzereigenschaft**.
   b) Klicken Sie unter **Eintragseigenschaften** auf **Auswählen**.
   c) Klicken Sie im Fenster **Objekteigenschaft wählen** auf **Vorname** in der Liste **Objekteigenschaft** und klicken Sie dann auf **OK**.
   d) Klicken Sie auf **OK**.
3. Klicken Sie auf **Hinzufügen**.
4. Konfigurieren Sie wie folgt den Eintrag so, dass er optional eine Eindeutigkeitszahl enthält:
   a) Klicken Sie unter **Eintragstyp** auf **Eindeutigkeitszahl**.
   b) Legen Sie unter **Eintragseigenschaften** wie folgt die Eintragsoptionen fest:
      - Klicken Sie auf **Hinzufügen, wenn Eigenschaftswert in Gebrauch ist**.
      - Aktivieren Sie das Kontrollkästchen **Zahl mit fester Länge und voranstehenden Nullen**.
      - Geben Sie in das Feld neben **Länge der Zahl in Stellen** den Wert **3** ein.
   c) Klicken Sie auf **OK**.
5. Klicken Sie auf **Hinzufügen**.
6. Konfigurieren Sie den Eintrag so, dass er einen Punkt enthält:
   a) Geben Sie im Bereich **Textwert** unter **Eintragseigenschaften** einen Punkt ein.
   b) Klicken Sie auf **OK**.

7. Klicken Sie auf **Hinzufügen**.
8. Konfigurieren Sie den Eintrag so, dass er den Nachnamen des Benutzers enthält:
   a) Klicken Sie unter **Eintragstyp** auf **Benutzereigenschaft**.
   b) Klicken Sie unter **Eintragseigenschaften** auf **Auswählen**.
   c) Klicken Sie im Fenster **Objekteigenschaft wählen** auf **Nachname** in der Liste **Objekteigenschaft** und klicken Sie dann auf **OK**.
   d) Klicken Sie auf **OK**.

Nach dem Ausführen dieser Schritte sollte die Liste der Einträge im Dialogfeld **Wert konfigurieren** der folgenden Abbildung ähneln.



Klicken Sie auf **OK**, um das **Dialogfeld Wert** konfigurieren zu schließen. Klicken Sie dann auf **Weiter** und befolgen Sie die Anweisungen im Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten für neues Bereitstellungsrichtlinienobjekt anwenden, oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen bezüglich der Anwendung eines Richtlinienobjekts finden Sie unter Anwenden von Richtlinienobjekten und Verwalten des Richtlinienbereichs weiter oben in diesem Kapitel.

Automatische Bereitstellung des Exchange-Postfachs

Richtlinien dieser Kategorie dienen zum Automatisieren der Auswahl eines Postfachspeichers oder einer Datenbank, wenn ein Benutzer in Microsoft Exchange Server für die Verwendung von Postfächern oder für die Erstellung eines Postfachs aktiviert wird.

Sie können Exchange-Server und Postfachspeicher oder Datenbanken mit zulässiger Postfacherstellung angeben sowie Regeln festlegen, um Postfächer auf mehrere Speicher zu verteilen. Beispielsweise können Sie eine Richtlinie so konfigurieren, dass sie automatisch einen der Speicher mit der geringsten Anzahl von Postfächern auswählt.

Funktionsweise dieser Richtlinie

Wenn ein Benutzer für die Verwendung oder Erstellung von Postfächern aktiviert wird, verwendet Quest One ActiveRoles diese Richtlinie, um den Postfachspeicher oder die Datenbank auszuwählen.
Die Richtlinie definiert einen einzelnen Speicher oder eine Gruppe von Speichern, wo die Erstellung von Postfächern zulässig ist. Es folgen einige spezifische Aspekte des Richtlinienverhaltens:

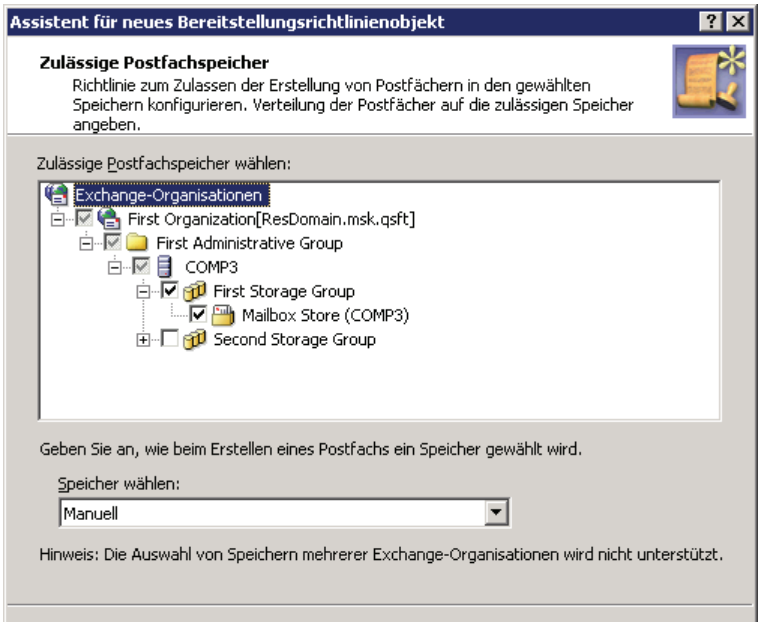
- Wenn die Richtlinie einen einzelnen Speicher angibt, werden Postfächer in diesem Speicher erstellt. Der Operator, der das Benutzerkonto erstellt oder aktualisiert, kann keinen anderen Speicher auswählen.
- Wenn die Richtlinie mehrere Speicher angibt, wird der Speicher automatisch (von Quest One ActiveRoles) oder manuell (von dem Operator, der das Benutzerkonto erstellt oder aktualisiert) ausgewählt, abhängig von den Richtlinienoptionen.

Im Fall mehrerer Speicher stellt die Richtlinie die folgenden Optionen bereit, um die Speicherauswahl zu steuern:

- **Manuell.** Ermöglicht es dem Operator, einen Speicher aus der von der Richtlinie definierten Liste auszuwählen.
- **Durch Anwendung des Kreisverfahrens.** Leitet Postfacherstellungs-Anforderungen sequenziell an die Speicher um. Dabei wird der erste Speicher für die erste Anforderung, der zweite Speicher für die zweite Anforderung verwendet usw. Nach dem Erreichen des letzten Speichers wird die nächste Anforderung an den ersten Speicher der Sequenz übergeben.
- **Mit der geringsten Zahl an Postfächern.** Leitet Anforderungen zur Erstellung von Postfächern an den Speicher weiter, der die geringste Anzahl von Postfächern enthält.

Konfigurieren der Richtlinie „Automatische Bereitstellung von Exchange-Postfächern"

Um die Richtlinie „Automatische Bereitstellung von Exchange-Postfächern" zu konfigurieren, wählen Sie **Automatische Bereitstellung von Exchange-Postfächern** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten für neues Bereitstellungsrichtlinienobjekt oder im Assistenten „Bereitstellungsrichtlinie hinzufügen" aus. Klicken Sie dann auf **Weiter**, um die Seite **Zulässige Postfachspeicher** anzuzeigen:


Assistent für neues Bereitstellungsrichtlinienobjekt
Zulässige Postfachspeicher
Richtlinie zum Zulassen der Erstellung von Postfächern in den gewählten Speichern konfigurieren. Verteilung der Postfächer auf die zulässigen Speicher angeben.
Zulässige Postfachspeicher wählen:
Exchange-Organisationen
First Organization[ResDomain.msk.qsft]
First Administrative Group
COMP3
First Storage Group
Mailbox Store (COMP3)
Second Storage Group
Geben Sie an, wie beim Erstellen eines Postfachs ein Speicher gewählt wird.
Speicher wählen:
Manuell
Hinweis: Die Auswahl von Speichern mehrerer Exchange-Organisationen wird nicht unterstützt.

Auf dieser Seite können Sie die Server und Postfachspeicher oder Datenbanken auswählen, die für die Postfacherstellung zulässig sein sollen. Wählen Sie Postfachspeicher aus einer einzelnen Exchange-Organisation aus. Das Auswählen von Postfachspeichern oder Datenbanken aus mehreren Organisationen wird nicht unterstützt.

Wenn Sie mehrere Speicher auswählen, können Sie angeben, wie bei einer Postfacherstellungsanforderung ein Speicher ausgewählt werden soll. Wählen Sie in der Liste **Speicher wählen** eine der folgenden Optionen aus, die weiter oben in diesem Abschnitt erörtert werden:

- Manuell
- Durch Anwendung des Kreisverfahrens
- Mit der geringsten Zahl an Postfächern

Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Verfahren zum Konfigurieren der Richtlinie „Automatische Bereitstellung von Exchange-Postfächern"

So konfigurieren Sie eine Richtlinie zur automatische Bereitstellung von Exchange-Postfächern:

1. Wählen Sie auf der Seite **Zu konfigurierende Richtlinie** die Option **Automatische Bereitstellung von Exchange-Postfächern** und klicken Sie dann auf **Weiter**.
2. Wählen Sie unter **Zulässige Postfachspeicher wählen** die Server und Speicherorte, die für die Erstellung von Postfächern zugelassen sind, und klicken anschließend auf **Weiter**.

   *Falls mehrere Speicher vorhanden sind, wählen Sie eine Methode zur Auswahl eines Speichers aus der Liste **Speicher wählen** aus. Weitere Informationen über die Verfahren zum Auswählen eines Speichers im Fall von mehreren Speichern finden Sie unter Funktionsweise dieser Richtlinie weiter oben in diesem Kapitel.*
3. Auf der Seite **Richtlinie erzwingen** können Sie Objekte angeben, auf die dieses Richtlinienobjekt angewandt werden soll:
   - Klicken Sie auf **Hinzufügen** und verwenden Sie das Objekt **Objekte auswählen**, um die gewünschten Objekte auszuwählen.
4. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Szenario: Lastenausgleich für Postfachspeicher

Mit der in diesem Szenario beschriebenen Richtlinie können mehrere Speicher für die Postfacherstellung verwendet werden, und Quest One ActiveRoles wählt automatisch den Speicher mit der kleinsten Anzahl von Postfächern aus.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie ein Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Wenn Sie ein Postfach für ein Benutzerkonto erstellen, das sich in dem in Schritt 2 ausgewählten Container befindet, wählt Quest One ActiveRoles daher aus den Speichern, in denen die Postfacherstellung zulässig ist, den am wenigsten ausgelasteten.

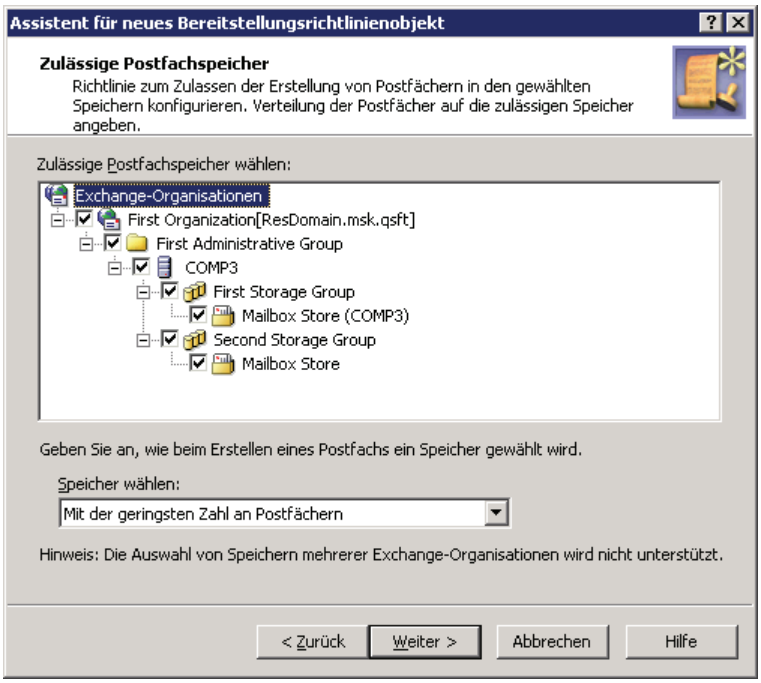
In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten für neues Bereitstellungsrichtlinienobjekt erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter Erstellen eines Richtlinienobjekts im Abschnitt Verwaltungsaufgaben für Richtlinienobjekte weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Richtlinientyp auswählen** des Assistenten auf **Automatische Bereitstellung von Exchange-Postfächern**. Klicken Sie dann auf **Weiter**.

Wählen Sie auf der Seite **Zulässige Postfachspeicher** die Speicher, in denen die Postfacherstellung zulässig sein soll. Klicken Sie dann unter **Speicher wählen** auf **Mit der geringsten Zahl an Postfächern**, wie in der folgenden Abbildung gezeigt.


Assistent für neues Bereitstellungsrichtlinienobjekt
Zulässige Postfachspeicher
Richtlinie zum Zulassen der Erstellung von Postfächern in den gewählten Speichern konfigurieren. Verteilung der Postfächer auf die zulässigen Speicher angeben.
Zulässige Postfachspeicher wählen:
Exchange-Organisationen
First Organization[ResDomain.msk.qsft]
First Administrative Group
COMP3
First Storage Group
Mailbox Store (COMP3)
Second Storage Group
Mailbox Store
Geben Sie an, wie beim Erstellen eines Postfachs ein Speicher gewählt wird.
Speicher wählen:
Mit der geringsten Zahl an Postfächern
Hinweis: Die Auswahl von Speichern mehrerer Exchange-Organisationen wird nicht unterstützt.
< Zurück
Weiter >
Abbrechen
Hilfe

Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten für neues Bereitstellungsrichtlinienobjekt anwenden, oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen bezüglich der Anwendung eines Richtlinienobjekts finden Sie unter Anwenden von Richtlinienobjekten und Verwalten des Richtlinienbereichs weiter oben in diesem Kapitel.

Standardmäßige Erstellungsoptionen für ein Exchange-Postfach

Im Assistenten für die Erstellung von Benutzerkonten – ganz gleich, ob in der Quest One ActiveRoles-Konsole oder im Web-Interface – ist die Option **Exchange-Postfach erstellen** standardmäßig ausgewählt, wodurch das Benutzerpostfach bei Erstellung eines Benutzerkontos erstellt wird. Dieses Verhalten kann durch Anwenden einer entsprechend entworfenen Richtlinie auf die Kategorie „Automatische Bereitstellung von Exchange-Postfächern" geändert werden.

Eine Richtlinie kann so konfiguriert werden, dass die Option **Exchange-Postfach erstellen** nicht standardmäßig ausgewählt ist, sondern der Administrator, der den Assistenten für die Erstellung eines Benutzerkontos verwendet, diese Option bei Bedarf auswählen kann. Es ist außerdem möglich, eine Richtlinie zu konfigurieren, die die Auswahl der Option **Exchange-Postfach erstellen** forciert.

Gehen Sie folgendermaßen vor, um standardmäßige Erstellungsoptionen für ein Exchange-Postfach festzulegen:

1. Erstellen Sie ein Richtlinienobjekt, das eine Richtlinie zur automatischen Bereitstellung von Exchange-Postfächern enthält.
2. Öffnen Sie das Dialogfeld **Eigenschaften** für das von Ihnen erstellte Richtlinienobjekt.
3. Doppelklicken Sie auf der Registerkarte **Richtlinien** im Dialogfeld **Eigenschaften** auf den Richtlinieneintrag „Automatische Bereitstellung von Exchange-Postfächern".
4. Legen Sie auf der Registerkarte **Postfacherstellung** im Dialogfeld **Eigenschaften der Richtlinie zur automatischen Bereitstellung von Exchange-Postfächern** Ihrer Situation entsprechende Richtlinienoptionen fest:
   - **Benutzerpostfach standardmäßig erstellen.** Legt fest, ob die Option **Exchange-Postfach erstellen** standardmäßig im Assistenten für die Erstellung von Benutzerkonten ausgewählt ist. Wenn der Benutzer Postfächer nicht standardmäßig erstellen soll, deaktivieren Sie diese Richtlinienoption.
   - **Erstellung des Postfachs erzwingen.** Führt dazu, dass die Option **Exchange-Postfach erstellen** ausgewählt und nicht verfügbar ist, sodass der Administrator, der ein Benutzerkonto erstellt, diese Option nicht deaktivieren kann.
5. Klicken Sie auf **OK**, um die von Ihnen geöffneten Dialogfelder zu schließen.
6. Wenden Sie das Richtlinienobjekt auf den Bereich an (Domänen, Container oder verwaltete Einheiten), in dem diese Richtlinie gelten soll.

Stammordner AutoProvisioning

Richtlinien dieser Kategorie automatisieren die Erstellung oder Umbenennung von Benutzerstammordnern und -stammfreigaben bei der Erstellung oder Umbenennung von Benutzerkonten mit Quest One ActiveRoles.

Sie können einen Server angeben, auf dem Stammordner und Stammfreigaben erstellt werden sollen. Sie können definieren, wie Berechtigungen für neue Stammordner und freigaben festgelegt werden. Sie können Namenskonventionen für neue Stammordner und Stammfreigaben angeben, und Sie können die Anzahl gleichzeitiger Verbindungen mit Stammfreigaben beschränken.

Beispielsweise kann mit Richtlinien dieses Typs eine Unternehmensregel definiert werden, mit der bei jeder Benutzerkontoerstellung in Quest One ActiveRoles auch ein Ordner in einer Netzwerkdateifreigabe erstellt und als Stammordner des Benutzers zugewiesen wird.

Funktionsweise dieser Richtlinie

Bei der Ausführung der Richtlinie zur automatische Bereitstellung von Stammordnern führt Quest One ActiveRoles diverse Aktionen aus, je nachdem, ob ein Benutzer erstellt, kopiert oder umbenannt wird.

Erstellen von Stammordnern und freigaben bei der Erstellung von Benutzerkonten

Wenn Quest One ActiveRoles ein Benutzerkonto erstellt (unabhängig davon, ob von Grund auf neu oder durch Kopieren eines vorhandenen Kontos), kann die Richtlinie dazu führen, dass Quest One ActiveRoles einen Stammordner und optional eine Stammfreigabe für das Konto, das den in der Richtlinie angegebenen Pfad nutzt, erstellt. Der Name der Stammfreigabe setzt sich aus dem Benutzernamen und dem in der Richtlinie angegebenen Präfix und Suffix zusammen.

Die Richtlinie bietet die Möglichkeit, die Erstellung von Stammordnern mit Pfaden und Namen, die sich von dem durch die Richtlinie vorgegebenen Pfad und Namen unterscheiden, zu aktivieren. Beispielsweise kann die Richtlinie „Erzeugung und Validierung von Eigenschaften" so konfiguriert werden, dass sie die Eigenschaften **Stammlaufwerk** und **Stammverzeichnis** für Benutzerkonten generiert. Wenn Sie Änderungen an diesen Eigenschaften vornehmen, prüft Quest One ActiveRoles, ob der angegebene Stammordner vorhanden ist, und erstellt gegebenenfalls den Stammordner.

In Quest One ActiveRoles ist eine spezielle Richtlinie implementiert, die die Ordner in Netzwerkdateifreigaben beschränkt, in denen Stammordner erstellt werden können. Das Richtlinienobjekt, das diese Richtlinie enthält, befindet sich im Container **Configuration/Policies/ Administration/Builtin**. Der Name des Richtlinienobjekts lautet **Built-in Policy – Home Folder Location Restriction**. Sie können es mit Hilfe der Quest One ActiveRoles-Konsole aufrufen. Die Richtlinieneinstellungen umfassen eine Liste der Ordner in den Netzwerkdateifreigaben, in denen die Erstellung von Stammordnern zulässig ist. Anweisungen bezüglich der Anzeige oder Änderung dieser Liste finden Sie unter „Konfigurieren der Richtlinie 'Einschränkungen bezüglich des Speicherorts von Stammordnern'" weiter unten in diesem Abschnitt.

Umbenennen von Stammordnern beim Umbenennen von Benutzerkonten

Wenn Quest One ActiveRoles den Benutzer-Anmeldenamen (Prä-Windows 2000) eines Benutzerkontos ändert, kann die Richtlinie den Stammordner umbenennen und optional die Stammfreigabe für dieses Benutzerkonto neu erstellen. Der Name der neuen Stammfreigabe wird gemäß den in der Richtlinie angegebenen Namenskonventionen erstellt.

Die Richtlinie benennt den vorhandenen Stammordner anhand des neuen Benutzer-Anmeldenamens (Prä-Windows 2000) um. Wenn der Stammordner allerdings gerade verwendet wird, kann Quest One ActiveRoles ihn nicht umbenennen. In diesem Fall erstellt Quest One ActiveRoles einen neuen Stammordner mit dem neuen Namen und verändert den vorhandenen Stammordner nicht.

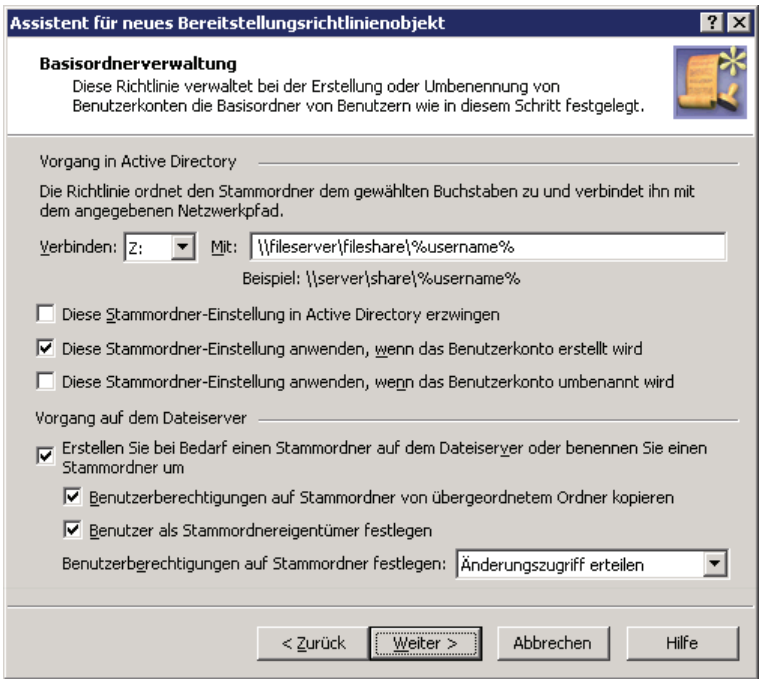
Option zur Vermeidung eines Vorgangs auf dem Dateiserver

Standardmäßig versucht Quest One ActiveRoles, einen (nicht lokalen) Stammordner auf dem Dateiserver zu erstellen oder umzubenennen, wenn die Eigenschaft „Stammverzeichnis" für ein Benutzerkonto in Active Directory gesetzt oder geändert wird. Wenn die Erstellung oder Umbenennung des Stammordners fehlschlägt (zum Beispiel weil der Zugriff auf den Dateiserver nicht möglich ist), dann schlägt die Erstellung oder Änderung des Benutzerkontos ebenfalls fehl. Um eine solche Fehlerbedingung zu vermeiden, kann eine Richtlinie für die automatische Bereitstellung von Stammordnern so konfiguriert werden, dass Quest One ActiveRoles die Änderungen auf die Eigenschaften **Home-Drive** und **Home-Directory** in Active Directory anwendet, ohne einen Vorgang auf dem Dateiserver zu versuchen. Diese Richtlinienoption ermöglicht die Verwendung eines anderen Tools als Quest One ActiveRoles für die Erstellung von Stammordnern auf dem Dateiserver.

Quest One ActiveRoles umfasst ein vorkonfiguriertes Richtlinienobjekt, das die Erstellung oder Umbenennung von Stammordnern bei der Festlegung von Stammordnereigenschaften für Benutzerkonten in Active Directory ermöglicht. Das Richtlinienobjekt befindet sich im Container **Configuration/Policies/Administration/Builtin** in der Quest One ActiveRoles-Konsolenstruktur. Der Name des Richtlinienobjekts lautet **Built-in Policy – Default Rules to Provision Home Folders**. Wenn Sie verhindern möchten, dass Quest One ActiveRoles versucht, Stammordner zu erstellen oder umzubenennen, können Sie die Richtlinie im integrierten Richtlinienobjekt ändern oder eine andere Richtlinie für die automatische Bereitstellung von Stammordnern erstellen und konfigurieren, bei der die entsprechende Option deaktiviert ist.

Konfigurieren der Richtlinie „Automatische Bereitstellung des Stammordners"

Um die Richtlinie „Automatische Bereitstellung des Stammordners" zu konfigurieren, wählen Sie **Automatische Bereitstellung des Stammordners** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten für neues Bereitstellungsrichtlinienobjekt oder im Assistenten „Bereitstellungsrichtlinie hinzufügen" aus. Klicken Sie dann auf **Weiter**, damit die Seite **Basisordnerverwaltung** angezeigt wird.


Assistent für neues Bereitstellungsrichtlinienobjekt
Basisordnerverwaltung
Diese Richtlinie verwaltet bei der Erstellung oder Umbenennung von Benutzerkonten die Basisordner von Benutzern wie in diesem Schritt festgelegt.
Vorgang in Active Directory
Die Richtlinie ordnet den Stammordner dem gewählten Buchstaben zu und verbindet ihn mit dem angegebenen Netzwerkpfad.
Verbinden: Z:
Mit: \\fileserver\fileshare\%username%
Beispiel: \\server\share\%username%
Diese Stammordner-Einstellung in Active Directory erzwingen
Diese Stammordner-Einstellung anwenden, wenn das Benutzerkonto erstellt wird
Diese Stammordner-Einstellung anwenden, wenn das Benutzerkonto umbenannt wird
Vorgang auf dem Dateiserver
Erstellen Sie bei Bedarf einen Stammordner auf dem Dateiserver oder benennen Sie einen Stammordner um
Benutzerberechtigungen auf Stammordner von übergeordnetem Ordner kopieren
Benutzer als Stammordnereigentümer festlegen
Benutzerberechtigungen auf Stammordner festlegen: Änderungszugriff erteilen
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite können Sie die folgenden Optionen konfigurieren.

Verbinden Sie <*Laufwerksbuchstabe*> mit <*Netzwerkpfad*>

Bei der Erstellung oder Umbenennung eines Benutzerkontos kann die Richtlinie das Benutzerkonto in Active Directory so konfigurieren, dass sie den Stammordner mit dem angegebenen Netzwerkpfad verbindet. Wählen Sie in der Liste **Verbinden** den Laufwerksbuchstabe des Laufwerks aus, dem die Richtlinie den Stammordner zuordnen soll. Geben Sie im Feld **An** einen Netzwerkpfad zum Stammordner ein. Vergewissern Sie sich, dass der Pfad den folgenden Anforderungen entspricht:

- Ein gültiger Netzwerkpfad muss mit dem UNC-Namen einer Netzwerkdateifreigabe wie etwa \\Server\Freigabe\ beginnen und normalerweise die Angabe %Benutzername% umfassen. Bei Auswahl der Richtlinieneinstellung **Verbinden: Z: Mit: \\Server\Freigabe\%Benutzername%** kann die Richtlinie ein Benutzerkonto in Active Directory so konfigurieren, dass die Eigenschaft **Home-Drive** des Benutzerkontos auf Z: und die Eigenschaft **Home-Directory** des Benutzerkontos auf \\Server\Freigabe\Anmeldename gesetzt ist, wobei „Anmeldename" für den PräWindows2000-Anmeldenamen des Benutzerkontos steht.
- Der Pfad muss eine gemeinsame Freigabe enthalten, die sich auf der Ebene direkt über den Stammordnern befindet. Wenn Sie beispielsweise **\\Comp\Home\%Benutzername%** eingeben, erstellt die Richtlinie Stammordner in der Netzwerkfreigabe **home** auf dem Server **comp**, wobei der Name des Ordners identisch mit dem Benutzeranmeldenamen (Prä Windows 2000) ist. Der Pfad **\\comp\%Benutzername%** ist ungültig.

- Der Ordner in der Netzwerkdateifreigabe, in der die Richtlinie Stammordner erstellen soll, muss in der Richtlinie „Einschränkungen bezüglich des Speicherorts von Stammordnern" aufgelistet sein. Anweisungen bezüglich der Anzeige oder Änderung der Liste finden Sie unter „Konfigurieren der Richtlinie 'Einschränkungen bezüglich des Speicherorts von Stammordnern'" weiter unten in diesem Abschnitt.
- Wenn Sie möchten, dass die Richtlinie Stammfreigaben erstellt (siehe Informationen über die Seite **Stammfreigabenverwaltung** weiter unten in diesem Abschnitt), dann dürfen Sie *keine* administrative Freigabe wie etwa C$ als die allgemeine Freigabe im Feld **Mit** angeben. Andernfalls kann die Richtlinie bei der Erstellung von Stammordnern möglicherweise keine Stammfreigaben erstellen. Wenn Sie also **\\Comp\C$\%Benutzername%** angeben, kann die Richtlinie erfolgreich Stammordner im Ordner **C:** auf dem Computer **Comp** erstellen, jedoch keine Stammfreigaben erstellen.

Diese Stammordner-Einstellung in Active Directory erzwingen

Verwenden Sie diese Option, damit Quest One ActiveRoles überprüft, ob de Eigenschaften **Stammlaufwerk** und **Stammverzeichnis** für Benutzerkonten in Active Directory mit der von dieser Richtlinie angegebenen Einstellung **Verbinden: <*Laufwerksbuchstabe*> Mit: <*Netzwerkpfad*>** konform ist.

Bei Auswahl der Richtlinieneinstellung **Verbinden: Z: Mit: \\Server\Freigabe\%Benutzername%** % führt diese Option beim Versuch, ein Benutzerkonto dahingehend zu ändern, dass der Eigenschaft **„Stammlaufwerk"** ein anderer Laufwerksbuchstabe als Z: zugewiesen wird, zu einem Richtlinienverstoß in Quest One ActiveRoles. Gleiches gilt, wenn der Eigenschaft **Home-Directory** ein anderer Netzwerkpfad als \\Server\Freigabe\Anmeldename zugewiesen wird, wobei „Anmeldename" für den Prä-Windows 2000-Anmeldenamen des Benutzerkontos steht.

Wenn diese Option deaktiviert ist, ermöglicht die Richtlinie, dass sich Stammordnerpfad und -name von dem durch die Richtlinie vorgegebenen Pfad und Namen unterscheiden. Es kann eine Richtlinie zur Erzeugung und Validierung von Eigenschaften konfiguriert werden, die die Eigenschaften **Stammlaufwerk** und **Stammverzeichnis** für Benutzerkonten erstellt. Diese Eigenschaften können auch manuell angegeben werden. In beiden Fällen aktualisiert Quest One ActiveRoles das Benutzerkonto, sodass der Ordner mit dem angegebenen Pfad und Namen als Stammordner des Benutzers festgelegt wird. Erforderlichenfalls erstellt Quest One ActiveRoles den Ordner.

Wenn diese Option aktiviert ist, verhält sich die Richtlinie wie folgt:

- Sie gewährleistet, dass der Pfad und der Name des Stammordners den Richtlinieneinstellungen entsprechen. Wenn bei der Erstellung oder Änderung eines Benutzerkontos ein anderer Pfad oder Name angegeben wird, ermöglicht die Richtlinie nicht das Senden des Stammordnerpfads und namens an das Verzeichnis.
- Der Befehl **Richtlinie prüfen** führt dazu, dass die Richtlinie die bestehenden Stammordnereinstellungen überprüft. Die Richtlinie überprüft die Ergebnisse über Richtlinienverstöße (falls vorhanden) und bietet die Möglichkeit, die Stammordnerpfad- und namenseinstellungen von Benutzerkonten zu korrigieren, damit diese den Richtlinieneinstellungen entsprechen.

Aktivieren Sie das Kontrollkästchen **Diese Stammordner-Einstellung in Active Directory erzwingen**, um zu gewährleisten, dass die Stammordner für Benutzerkonten entsprechend dieser Richtlinie eingerichtet werden.

Wenn Sie das Kontrollkästchen deaktivieren, haben Sie die Möglichkeit, die Richtlinie „Erzeugung und Validierung von Eigenschaften" anzuwenden, um die Eigenschaften „Stammlaufwerk" und „Stammverzeichnis" zu generieren und zu validieren. In diesem Fall erstellt Quest One ActiveRoles Stammordner in Übereinstimmung mit den flexiblen, in hohem Maß anpassbaren Richtlinienregeln, die von der Richtlinie „Erzeugung und Validierung von Eigenschaften" bereitgestellt werden, und ordnet diese dem Stammordner zu.

Wenn Sie die Eigenschaften **Stammlaufwerk** und **Stammverzeichnis** festlegen, erstellt Quest One ActiveRoles den Stammordner nicht, wenn der Netzwerkpfad zu dem Ordner, in dem sich der Stammordner befinden soll, nicht in der Richtlinie Einschränkung bezüglich des Speicherorts des Stammordners aufgelistet ist. Die Richtlinie definiert eine Liste zu den Ordnern in Netzwerkdateifreigaben, in denen die Erstellung von Stammordnern zulässig ist, und verhindert, dass Quest One ActiveRoles Stammordner an anderen Netzwerkspeicherplätzen erstellt. Anweisungen bezüglich der Anzeige oder Änderung dieser Richtlinieneinstellungen finden Sie unter „Konfigurieren der Richtlinie 'Einschränkungen bezüglich des Speicherorts von Stammordnern'" weiter unten in diesem Abschnitt.

Diese Stammordner-Einstellung anwenden, wenn das Benutzerkonto erstellt wird

Bei Erstellung eines Benutzerkontos führt diese Option dazu, dass Quest One ActiveRoles das Benutzerkonto in Active Directory so konfiguriert, dass es mit der durch diese Richtlinie festgelegten Einstellung **Verbinden: *<Laufwerksbuchstabe>* Mit: *<Netzwerkpfad>*** konform ist.

Bei Auswahl der Richtlinieneinstellung **Verbinden: Z: Mit: \\Server\Freigabe\%Benutzername%** dazu, dass die Aktivierung dieses Kontrollkästchens gewährleistet, dass die Eigenschaft **Stammverzeichnis** für ein neu erstelltes Benutzerkonto auf Z: und die Eigenschaft **„Stammverzeichnis"** auf \\Server\Freigabe\Anmeldename gesetzt ist, wobei „Anmeldename" für den Prä-Windows 2000-Anmeldenamen des Benutzerkontos steht.

Diese Stammordner-Einstellung anwenden, wenn das Benutzerkonto umbenannt wird

Beim Umbenennen eines Benutzerkontos führt diese Option dazu, dass Quest One ActiveRoles das Benutzerkonto in Active Directory so konfiguriert, dass es mit der durch diese Richtlinie festgelegten Einstellung **Verbinden: *<Laufwerksbuchstabe>* Mit: *<Netzwerkpfad>*** konform ist.

Bei Auswahl der Richtlinieneinstellung **Verbinden: Z: Mit: \\Server\Freigabe\%Benutzername%** beispielsweise führt die Umbenennung eines Benutzerkontos dazu, dass die Richtlinie die Eigenschaft **„Stammverzeichnis"** auf \\Server\Freigabe\NeuerAnmeldename setzt, wobei „NeuerAnmeldename" für den Prä-Windows 2000-Anmeldenamen steht, der dem Benutzerkonto durch den Umbenennungsvorgang zugewiesen wird.

Erstellen Sie bei Bedarf einen Stammordner auf dem Dateiserver oder benennen Sie einen Stammordner um

Ist diese Option ausgewählt, so weist Sie Quest One ActiveRoles an, die Erstellung oder Umbenennung eines (nicht lokalen) Stammordners auf dem Dateiserver zu versuchen, wenn die Eigenschaft **Stammverzeichnis** für ein Benutzerkonto in Active Directory gesetzt oder geändert wird. Die Umbenennung des Stammordners wird versucht, wenn der Eigenschaftswert **„Stammverzeichnis"** die Angabe %Benutzername% enthält und die Änderungen am Benutzerkonto die Änderung des Prä-Windows 2000-Anmeldenamens des Benutzerkontos umfasst. In allen anderen Fällen wird versucht, einen neuen Stammordner zu erstellen.

Bei Auswahl der Richtlinieneinstellung **Verbinden: Z: Mit: \\Server\Freigabe\%Benutzername%** und Aktivierung dieses Kontrollkästchens zusammen mit der Option zur Anwendung der Richtlinieneinstellung bei Erstellung eines BenutzerkontosQuest One ActiveRoles, den Stammordner für das Benutzerkonto zu erstellen. Quest One ActiveRoles versucht, den Ordner mit dem folgenden Netzwerkpfad zu erstellen: \\Server\Freigabe\Anmeldename, wobei „Anmeldename" für den Prä-Windows 2000-Anmeldenamen des Benutzerkontos steht.

Ein weiteres Beispiel ist die Konfiguration der Eigenschaften **Stammlaufwerk** und **Stammverzeichnis** für ein vorhandenes Benutzerkonto in Active Directory: Bei Aktivierung dieses Kontrollkästchens versucht Quest One ActiveRoles, den Ordner zu erstellen, der durch den Netzwerkpfad angegeben ist, der der Eigenschaft **Stammverzeichnis** zugewiesen ist.

Wenn die Erstellung oder Umbenennung des Stammordners auf dem Dateiserver fehlschlägt, dann schlägt die Erstellung oder Änderung des Benutzerkontos ebenfalls fehl. Um eine solche Fehlerbedingung zu vermeiden, können Sie dieses Kontrollkästchen deaktivieren. Dies führt dazu, dass Quest One ActiveRoles die Änderungen auf die Eigenschaften **Stammlaufwerk** und **Stammverzeichnis** in Active Directory anwendet, ohne einen Vorgang auf dem Dateiserver zu unternehmen, was die Verwendung eines anderen Tools für die Erstellung von Stammordnern auf dem Dateiserver ermöglicht.

Benutzerberechtigungen auf Stammordner von übergeordnetem Ordner kopieren

Bei der Erstellung oder Umbenennung eines Stammordners für ein bestimmtes Benutzerkonto gewährleistet diese Option, dass das Benutzerkonto über dieselben Rechte in Bezug auf den Stammordner verfügt, die es auch in Bezug auf den Ordner hat, in dem sich der Stammordner befindet.

Benutzer als Stammordnereigentümer festlegen

Bei der Erstellung oder Umbenennung eines Stammordners für ein bestimmtes Benutzerkonto gewährleistet diese Option, dass das Benutzerkonto als Besitzer des Stammordners festgelegt wird.

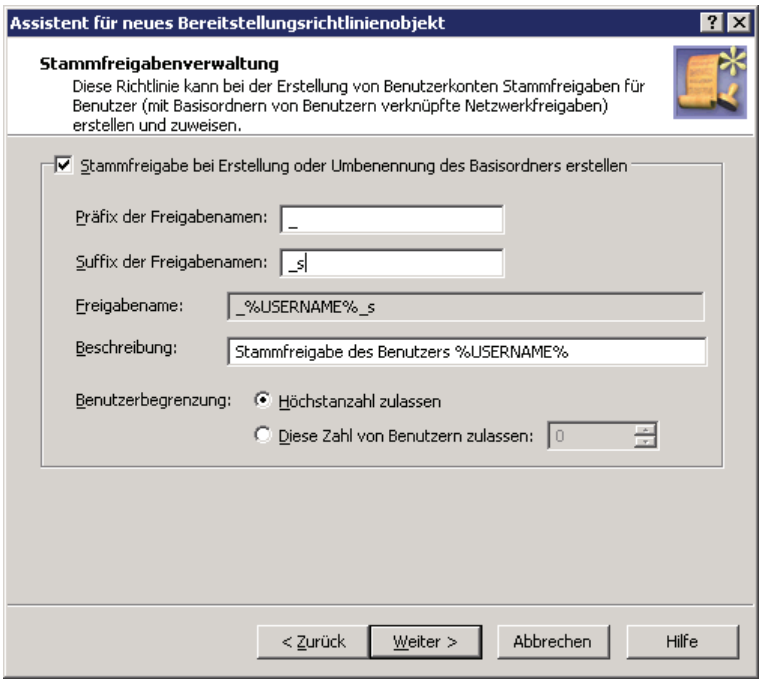
Ein Besitzer eines Ordners ist autorisiert, beliebige Änderungen an den Berechtigungseinstellungen für den Ordner durchzuführen. Ein Besitzer kann zum Beispiel anderen Personen den Zugriff auf den Ordner gewähren.

Benutzerberechtigungen für Stammordner festlegen

Bei der Erstellung oder Umbenennung eines Stammordners für ein bestimmtes Benutzerkonto gewährleistet diese Option, dass das Benutzerkonto über die spezifischen Zugriffsrechte für den Stammordner verfügt.

Mit der Einstellung **Vollzugriff erteilen** ist das Benutzerkonto autorisiert, jegliche Vorgänge am Ordner und seinen Inhalten durchzuführen. Ausnahme: Änderungen an den Berechtigungseinstellungen. Bei Aktivierung der Option **Änderungszugriff erteilen** ist das Benutzerkonto autorisiert, den Inhalt des Ordners anzuzeigen und zu ändern.

Klicken Sie danach auf **Weiter**, um die Seite **Stammfreigabenverwaltung** anzuzeigen. Auf dieser Seite können Sie Richtlinienoptionen für die Erstellung von Stammfreigaben konfigurieren:


Assistent für neues Bereitstellungsrichtlinienobjekt
Stammfreigabenverwaltung
Diese Richtlinie kann bei der Erstellung von Benutzerkonten Stammfreigaben für Benutzer (mit Basisordnern von Benutzern verknüpfte Netzwerkfreigaben) erstellen und zuweisen.
Stammfreigabe bei Erstellung oder Umbenennung des Basisordners erstellen
Präfix der Freigabenamen: _
Suffix der Freigabenamen: _s
Freigabename: _%USERNAME%_s
Beschreibung: Stammfreigabe des Benutzers %USERNAME%
Benutzerbegrenzung: Höchstanzahl zulassen
Diese Zahl von Benutzern zulassen: 0
< Zurück
Weiter >
Abbrechen
Hilfe

Damit die Richtlinie Stammfreigaben erstellt, aktivieren Sie das Kontrollkästchen **Stammfreigabe bei Erstellung oder Umbenennung des Basisordners erstellen**.

Wenn Sie die Richtlinie für die Erstellung von Stammfreigaben konfigurieren, können Sie das Präfix und Suffix für die Stammfreigabenamen angeben.

Indem Sie ein Präfix und Suffix angeben, können Sie eine Namenskonvention für Stammfreigaben einrichten. Nehmen Sie beispielsweise an, dass Sie Stammfreigaben ganz oben in der Freigabenliste anzeigen möchten. Verwenden Sie dazu als Präfix einen Unterstrich. Sie können auch ein Suffix zuweisen, um von der Richtlinie erstellte Stammfreigaben besonders zu kennzeichnen. Um beispielsweise die Stammfreigaben von Benutzern aus der Sales-Abteilung zu kennzeichnen, können Sie das Suffix _s verwenden. Wenn Sie nun ein Benutzerkonto mit dem Benutzer-Anmeldenamen JohnB (Prä-Windows 2000) erstellen, ordnet die Richtlinie den Stammordner des Benutzers dem ausgewählten Laufwerk zu und gibt **\\Server_JohnB_s** als Pfad zum Stammordner an. Die Richtlinie erstellt außerdem die Freigabe _**JohnB_s**, die auf den Ordner **\\Server\Home\JohnB** zeigt.

Optional können sie in das Feld **Beschreibung** einen Kommentar zu der Stammfreigabe eingeben. Dieser ist für die Benutzer sichtbar, wenn sie Freigabeeigenschaften anzeigen.

Sie können auch die Anzahl der Benutzer begrenzen, die gleichzeitig eine Verbindung mit der Freigabe herstellen können. Klicken Sie dazu auf **Höchstanzahl zulassen** oder **Diese Zahl von Benutzern zulassen**. Geben Sie bei der letzteren Option in das Feld neben der Option eine Zahl ein.

Verfahren zum Konfigurieren einer Richtlinie für die automatische Bereitstellung von Stammordnern

So konfigurieren Sie eine Richtlinie für die automatische Bereitstellung von Stammordnern:

1. Wählen Sie auf der Seite **Zu konfigurierende Richtlinie** die Option **Automatische Bereitstellung des Stammordners** aus und klicken Sie dann auf **Weiter**.
2. Gehen Sie auf der Seite **Basisordnerverwaltung** wie nachfolgend beschrieben vor und klicken Sie dann auf **Weiter**:
   - Wählen Sie in der Liste **Verbinden** den Laufwerksbuchstabe des Laufwerks aus, dem die Richtlinie den Stammordner zuordnen soll.
   - Geben Sie im Feld **An** einen Netzwerkpfad zum Stammordner ein.

   Der Pfad muss eine gemeinsame Freigabe enthalten, die sich auf der Ebene direkt über den Stammordnern befindet. So können Sie zum Beispiel \\Ant\Home\%Benutzername% angeben, damit die Richtlinie Stammordner in der Freigabe „Home" auf dem Server „Ant." erstellt. Ein Pfad wie etwa \\SERVER\%Benutzername% ist ungültig.

   - Damit die Richtlinie überprüft, ob der Stammordnerpfad und name von Benutzerkonten in Übereinstimmung mit dieser Richtlinie festgelegt wurden, wählen Sie **Diese Stammordnereinstellung in Active Directory erzwingen**.

   Wenn dieses Kontrollkästchen deaktiviert ist, ermöglicht die Richtlinie die Erstellung von Stammordnern mit Pfaden und Namen, die sich von dem durch die Richtlinie vorgegebenen Pfad und Namen unterscheiden.

   - Damit Quest One ActiveRoles die Stammordnereigenschaften bei der Erstellung eines Benutzerkontos in Active Directory automatisch in Übereinstimmung mit dieser Richtlinie festlegt, wählen Sie **Diese Stammordnereinstellung bei Einstellung des Benutzerkontos anwenden**.
   - Damit Quest One ActiveRoles die Stammordnereigenschaften bei der Umbenennung eines Benutzerkontos in Active Directory automatisch in Übereinstimmung mit dieser Richtlinie festlegt, wählen Sie **Diese Stammordnereinstellung bei Umbenennung des Benutzerkontos anwenden**.
   - Damit Quest One ActiveRoles versucht, einen (nicht lokalen) Stammordner auf dem Dateiserver zu erstellen oder umzubenennen, wenn die Stammordnereigenschaften für ein Benutzerkonto in Active Directory festgelegt oder geändert werden, aktivieren Sie die Option **Stammverzeichnis auf Dateiserver bei Bedarf erstellen oder umbenennen**.

   *Wenn Sie die Richtlinie so konfigurieren möchten, dass sie nicht nur die Stammordner-Eigenschaften für Benutzerkonten in Active Directory festlegt, sondern auch Stammordner und Stammfreigaben in Übereinstimmung mit den Richtlinieneinstellungen erstellt oder umbenennt, müssen Sie das Kontrollkästchen **Stammverzeichnis auf Dateiserver bei Bedarf erstellen oder umbenennen** aktiviert lassen (dies ist die Standardeinstellung). Wenn das Kontrollkästchen deaktiviert wird, dann kann die Richtlinie nur Stammordner-Eigenschaften für Benutzerkonten in Active Directory festlegen oder überprüfen.*

   - Geben Sie an, wie die Richtlinie Berechtigungseinstellungen für Stammordner konfigurieren soll. Sie können unter den folgenden Optionen wählen:
     - **Benutzerberechtigungen auf Stammordner von übergeordnetem Ordner kopieren.** Bei der Erstellung oder Umbenennung eines Stammordners für ein Benutzerkonto gewährleistet diese Option, dass das Benutzerkonto über dieselben Rechte in Bezug auf den Stammordner verfügt, die es auch in Bezug auf den Ordner hat, in dem sich der Stammordner befindet.
     - **Benutzer als Stammordnereigentümer festlegen.** Bei der Erstellung oder Umbenennung eines Stammordners für ein Benutzerkonto gewährleistet diese Option, dass das Benutzerkonto als Besitzer des Stammordners festgelegt wird.
     - **Benutzerberechtigungen für Stammordner festlegen.** Bei der Erstellung oder Umbenennung eines Stammordners für ein Benutzerkonto gewährleistet diese Option, dass das Benutzerkonto über die spezifischen Zugriffsrechte für den Stammordner verfügt (wie etwa „Zugriff ändern" oder „Vollzugriff").

3. Legen Sie auf der Seite **Stammfreigabenverwaltung** die Einstellungen für die Benutzerstammfreigaben fest. Gehen Sie folgendermaßen vor und klicken Sie dann auf **Weiter**:
   - Wählen Sie **Stammfreigabe bei Erstellung oder Umbenennung des Stammordners erstellen**, damit die Richtlinie die Stammfreigabe bei der Erstellung oder beim Umbenennen des Stammordners erstellt oder umbenennt.
   - Geben Sie optional unter **Präfix der Stammfreigabe** und **Suffix der Stammfreigabe** einen Präfix und Suffix für den Namen der Stammfreigabe ein. Ausführlichere Informationen finden Sie im Abschnitt Konfigurieren der Richtlinie „Automatische Bereitstellung des Stammordners" weiter oben in diesem Kapitel.
   - Optional können Sie in das Feld **Beschreibung** einen Kommentar eingeben, der zur Stammfreigabe hinzugefügt werden soll.
   - Wenn Sie die Anzahl der Benutzer, die gleichzeitig eine Verbindung zu der Freigabe herstellen können, einschränken möchten, klicken Sie auf **Diese Zahl von Benutzern zulassen** und geben Sie die maximale Anzahl der Benutzer in das Feld neben dieser Option ein. Klicken Sie andernfalls auf **Höchstanzahl zulassen**.
4. Auf der Seite **Richtlinie erzwingen** können Sie Objekte angeben, auf die dieses Richtlinienobjekt angewandt werden soll:
   - Klicken Sie auf **Hinzufügen** und verwenden Sie das Objekt **Objekte auswählen**, um die gewünschten Objekte auszuwählen.
5. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Weitere Informationen über die Konfigurationsoptionen der Richtlinie für die automatische Bereitstellung von Stammordnern finden Sie unter Konfigurieren der Richtlinie „Automatische Bereitstellung des Stammordners" weiter oben in diesem Kapitel.

Verwenden der integrierten Richtlinie für die Bereitstellung des Stammordners

Wenn Sie Quest One ActiveRoles so konfigurieren möchten, dass die Festlegung oder Änderung von mit dem Stammordner in Verbindung stehenden Eigenschaften für ein beliebiges Benutzerkonto in einer beliebigen verwalteten Domäne nicht zu dem Versuch der Erstellung oder Umbenennung eines Ordners auf einem Dateiserver führt, dann können Sie die Quest One ActiveRoles-Konsole verwenden, um das integrierte Richtlinienobjekt zu ändern:

1. Wählen Sie in der Konsolenstruktur **Configuration | Policies | Administration | Builtin**.
2. Doppelklicken Sie im Bereich „Details" auf **Built-in Policy – Default Rules to Provision Home Folders**.
3. Wählen Sie auf der Registerkarte **Richtlinien** die Richtlinie aus der Liste aus und klicken Sie dann auf **Anzeigen/Bearbeiten**.
4. Deaktivieren Sie auf der Registerkarte **Stammordner** das Kontrollkästchen **Erstellen Sie bei Bedarf einen Stammordner auf dem Dateiserver oder benennen Sie einen Stammordner um**.
5. Klicken Sie auf **OK**, um die von Ihnen geöffneten Dialogfelder zu schließen.

Wenn Sie über andere Richtlinienobjekte verfügen, die Richtlinien der Kategorie „Automatische Stammordner-Bereitstellung" enthalten, dann müssen Sie sie entsprechend konfigurieren: Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Erstellen Sie bei Bedarf einen Stammordner auf dem Dateiserver oder benennen Sie einen Stammordner um** in jeder dieser Richtlinien abhängig davon, ob Quest One ActiveRoles die Erstellung oder Umbenennung von Stammordnern für Benutzerkonten versuchen soll, die in den Bereich des entsprechenden Richtlinienobjekts fallen.

In einer anderen Situation kann es erforderlich sein, dass Quest One ActiveRoles Stammordner für Benutzerkonten erstellen oder umbenennen soll, die sich außerhalb eines bestimmten Bereichs befinden (wie etwa eine bestimmte Domäne, Organisationseinheit oder verwaltete Einheit), wobei die Erstellung oder Umbenennung von Stammordnern nicht für Benutzerkonten versucht werden soll, die in diesen bestimmten Bereich fallen. In diesem Szenario müssen Sie sicherstellen, dass die Option **Erstellen Sie bei Bedarf einen Stammordner auf dem Dateiserver oder benennen Sie einen Stammordner um** im integrierten Richtlinienobjekt ausgewählt ist. Dann müssen Sie ein Richtlinienobjekt erstellen und konfigurieren, das eine Richtlinie der Kategorie „Automatische Stammordner-Bereitstellung" mit deaktivierter Option **Erstellen Sie bei Bedarf einen Stammordner auf dem Dateiserver oder benennen Sie einen Stammordner um** enthält, und dieses Richtlinienobjekt dann auf den betreffenden Bereich anwenden.

Konfigurieren der Richtlinie „Einschränkungen bezüglich des Speicherorts von Stammordnern"

Bei der Erstellung von Stammordnern arbeitet Quest One ActiveRoles im Sicherheitskontext des Dienstkontos, unter dem der Verwaltungsdienst ausgeführt wird. Daher muss das Dienstkonto über ausreichende Rechte zur Erstellung von Stammordnern verfügen. Normalerweise hat das Dienstkonto administrative Rechte für den gesamten Dateiserver, was es Quest One ActiveRoles ermöglicht, Stammordner in jedem beliebigen Ordner in jeder Netzwerkdateifreigabe zu erstellen, die auf diesem Server existiert. Die Richtlinie „Einschränkung bezüglich des Speicherorts des Stammordners" wird verwendet, um die Netzwerkdateifreigaben und -ordner, in denen Quest One ActiveRoles Stammordner erstellen darf, auf eine bestimmte Liste zu beschränken.

Die Richtlinie „Einschränkung bezüglich des Speicherorts des Stammordners" legt die Ordner in den Netzwerkdateifreigaben fest, in denen Quest One ActiveRoles Stammordner erstellen darf, und verhindert, dass Quest One ActiveRoles Stammordner an anderen Speicherpositionen erstellt. Die von dieser Richtlinie auferlegten Einschränkungen gelten nicht, wenn die Erstellung des Stammordners von einem Inhaber der Rolle „ActiveRoles-Admin" durchgeführt wird (normalerweise sind dies die Benutzer, die Mitglied in der lokalen Administratorengruppe auf dem Computer sind, auf dem der Quest One ActiveRoles Verwaltungsdienst ausgeführt wird). Wenn als ein Inhaber der Rolle „ActiveRoles-Admin" ein Benutzerkonto erstellt und eine bestimmte Richtlinie zur Erleichterung der Bereitstellung von Stammordnern gültig ist, wird der Stammordner unabhängig von den Einstellungen der Richtlinie „Einschränkung bezüglich des Speicherorts des Stammordners" erstellt.

Standardmäßig sind keine Netzwerkdateifreigaben und ordner in der Richtlinie aufgelistet. Das bedeutet, dass Quest One ActiveRoles keinen Stammordner erstellen kann, sofern der Benutzerverwaltungsvorgang, der die Erstellung des Stammordners umfasst, nicht von einem Inhaber der Rolle „ActiveRoles-Admin" durchgeführt wird. Um delegierten Administratoren die Erstellung von Stammordnern zu ermöglichen, müssen Sie die Richtlinie so konfigurieren, dass sie die Ordner in den Netzwerkdateifreigaben auflistet, in denen die Erstellung von Stammordnern zulässig ist. Führen Sie hierzu das nachfolgend beschriebene Verfahren mit Hilfe der Quest One ActiveRoles-Konsole aus:

Gehen Sie folgendermaßen vor, um die Richtlinie „Einschränkung bezüglich des Speicherorts des Stammordners" zu konfigurieren:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Policies | Administration** und wählen Sie dann **Builtin** unter **Administration**
2. Doppelklicken Sie im Bereich „Details" auf **Built-in Policy – Home Folder Location Restriction**.

3. Doppelklicken Sie auf der Registerkarte **Richtlinien** auf das Listenelement unter **Richtlinienbeschreibung**.
4. Zeigen Sie auf der Registerkarte **Zulässige Speicherorte** die Liste der Ordner in den Netzwerkdateifreigaben an, in denen die Erstellung von Stammordnern zulässig ist, oder ändern Sie diese Liste.

   Wenn sie einen Ordner zur Liste hinzufügen, geben Sie den UNC-Name des Ordners an. Wenn Sie den Namen in der Form \\<Server>\<Freigabe> angeben, können Stammordner in jedem beliebigen Ordner in der angegebenen Netzwerkdateifreigabe erstellt werden. Wenn Sie den Namen in der Form \\<Server>\<Freigabe>\<PfadZumOrdner> angeben, können Stammordner in jedem beliebigen Unterordner des Ordners in der Netzwerkfreigabe erstellt werden.

Szenario: Erstellen und Zuweisen von Stammordnern

In diesem Szenario konfigurieren Sie eine Richtlinie, mit der bei der Erstellung von Benutzerkonten auch Stammordner erstellt werden. Die Richtlinie weist neu erstellten Konten Stammordner zu und gewährt den Benutzern Änderungszugriff auf ihre Stammordner.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Überprüfen Sie, ob die Netzwerkdateifreigabe, in der die Richtlinie Stammordner erstellen soll, in der Richtlinie Einschränkung bezüglich des Speicherorts des Stammordners aufgelistet ist.
2. Erstellen und konfigurieren Sie ein Richtlinienobjekt, das die entsprechende Richtlinie definiert.
3. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Wenn Sie in dem in Schritt 3 ausgewählten Container ein Benutzerkonto erstellen, erstellt Quest One ActiveRoles folglich den Benutzerstammordner und weist ihn dem Benutzerkonto zu.

In den folgenden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Überprüfen der Richtlinie „Einschränkung bezüglich des Speicherorts des Stammordners"

Die Netzwerkdateifreigabe, in der sich die Stammordner befinden sollen, muss in der Richtlinie „Einschränkung bezüglich des Speicherorts des Stammordners" aufgeführt sein. Befolgen Sie die Anweisungen unter „Konfigurieren der Richtlinie 'Einschränkungen bezüglich des Speicherorts von Stammordnern'", um zu überprüfen, dass die Richtlinie die Erstellung von Stammordnern in der Netzwerkdateifreigabe zulässt.

Schritt 2: Erstellen und Konfigurieren des Richtlinienobjekts

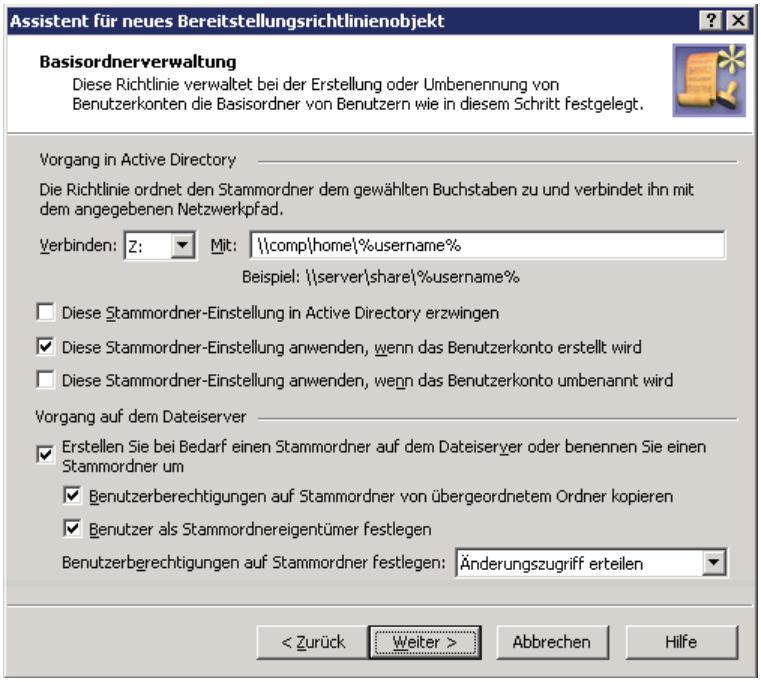
Sie können das benötigte Richtlinienobjekt mit dem Assistenten für neues Bereitstellungsrichtlinienobjekt erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter Erstellen eines Richtlinienobjekts im Abschnitt Verwaltungsaufgaben für Richtlinienobjekte weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Zu konfigurierende Richtlinie** des Assistenten auf **Automatische Bereitstellung des Stammordners**. Klicken Sie dann auf **Weiter**.

Richten Sie auf der Seite **Basisordnerverwaltung** folgende Optionen ein:

- Wählen Sie im Feld **Verbinden** den Laufwerksbuchstaben aus, der dem Stammordner zugewiesen werden soll. Sie können beispielsweise **Z: auswählen.**
- Geben Sie in das Feld **Mit** den Pfad in der Formular \\server\share\%username% ein, wobei \\Server\Freigabe ein gültiger UNC-Pfad zu einer Netzwerkdateifreigabe ist. Wenn Sie beispielsweise auf dem Server **comp** eine Netzwerkdateifreigabe eingerichtet haben, deren Freigabename auf **home** gesetzt ist, können Sie folgenden Pfad angeben: \\comp\home\%username%
- Aktivieren Sie das Kontrollkästchen **Diese Stammordner-Einstellung anwenden, wenn das Benutzerkonto erstellt wird**.

Nunmehr sollte die Seite **Basisordnerverwaltung** der folgenden Abbildung entsprechen.


Assistent für neues Bereitstellungsrichtlinienobjekt
Basisordnerverwaltung
Diese Richtlinie verwaltet bei der Erstellung oder Umbenennung von Benutzerkonten die Basisordner von Benutzern wie in diesem Schritt festgelegt.
Vorgang in Active Directory
Die Richtlinie ordnet den Stammordner dem gewählten Buchstaben zu und verbindet ihn mit dem angegebenen Netzwerkpfad.
Verbinden: Z:
Mit: \\comp\home\%username%
Beispiel: \\server\share\%username%
Diese Stammordner-Einstellung in Active Directory erzwingen
Diese Stammordner-Einstellung anwenden, wenn das Benutzerkonto erstellt wird
Diese Stammordner-Einstellung anwenden, wenn das Benutzerkonto umbenannt wird
Vorgang auf dem Dateiserver
Erstellen Sie bei Bedarf einen Stammordner auf dem Dateiserver oder benennen Sie einen Stammordner um
Benutzerberechtigungen auf Stammordner von übergeordnetem Ordner kopieren
Benutzer als Stammordnereigentümer festlegen
Benutzerberechtigungen auf Stammordner festlegen: Änderungszugriff erteilen
< Zurück
Weiter >
Abbrechen
Hilfe

Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 3: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten für neues Bereitstellungsrichtlinienobjekt anwenden, oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten. Weitere Informationen bezüglich der Anwendung eines Richtlinienobjekts finden Sie unter Anwenden von Richtlinienobjekten und Verwalten des Richtlinienbereichs weiter oben in diesem Kapitel.

Skriptausführung

Richtlinien dieser Kategorie dienen der Ausführung ergänzender Skripts auf Anforderung zur Ausführung administrativer Vorgänge.

Richtlinien, die auf der Ausführung benutzerdefinierter Skripts basieren, können Datenformate und anforderungen regulieren, Verwaltungsaufgaben automatisieren sowie zusätzliche Aktionen auslösen, um die Kontenbereitstellung zu automatisieren. Sie können ein benutzerdefiniertes Skript einem administrativen Vorgang zuordnen und Quest One ActiveRoles das Skript ausführen lassen, wenn der Vorgang angefordert wird oder nachdem er abgeschlossen wurde.

Betrachten Sie beispielsweise einen Benutzer, der von Seattle nach Atlanta versetzt wird. Sie können ein Skript schreiben, das den Benutzer von der Organisationseinheit Seattle in die Organisationseinheit Atlanta verschiebt, wenn das Attribut für die Stadt im Benutzerkonto aktualisiert wird.

Funktionsweise dieser Richtlinie

Quest One ActiveRoles führt das in der Richtlinie angegebene Skriptmodul aus, wenn der Vorgang angefordert wird oder nachdem er abgeschlossen wurde. Das Skriptmodul wird in der Konfigurationsdatenbank von Quest One ActiveRoles gespeichert.

Konfigurieren der Richtlinie „Skriptausführung"

Beim Konfigurieren der Richtlinie „Skriptausführung" können Sie vorab ein Skriptmodul vorbereiten. Alternativ können Sie auch beim Konfigurieren einer Richtlinie ein leeres Skriptmodul erstellen und dieses später bearbeiten, um ein von der Richtlinie zu verwendendes Skript hinzuzufügen.

Sie können ein Skript aus einer Datei importieren oder mit Hilfe der Quest One ActiveRoles-Konsole ein neues Skript schreiben. Die Konsole zeigt Skriptmodule im Container **Script Modules** unter **Configuration** an.

Importieren eines Skripts

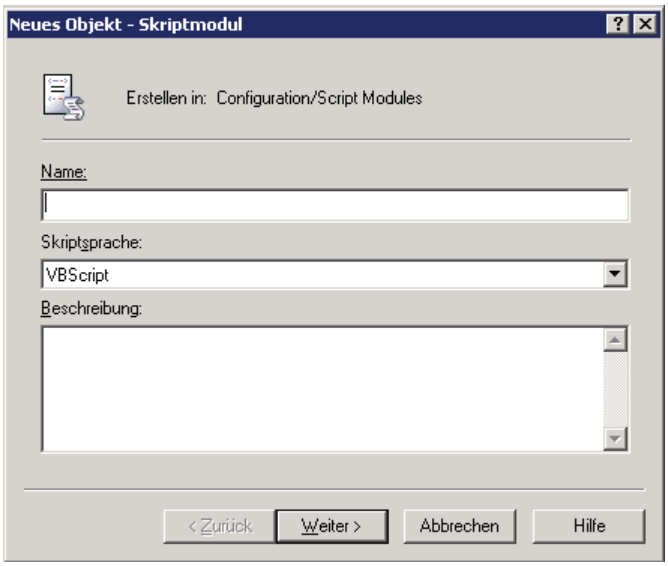
Klicken Sie zum Importieren einer Skriptdatei in der Konsolenstruktur mit der rechten Maustaste auf **Script Modules** und klicken Sie dann auf **Importieren**. Dann wird das Dialogfeld **Skript importieren** angezeigt, in dem Sie eine Skriptdatei auswählen und öffnen können.

Erstellen eines Skripts

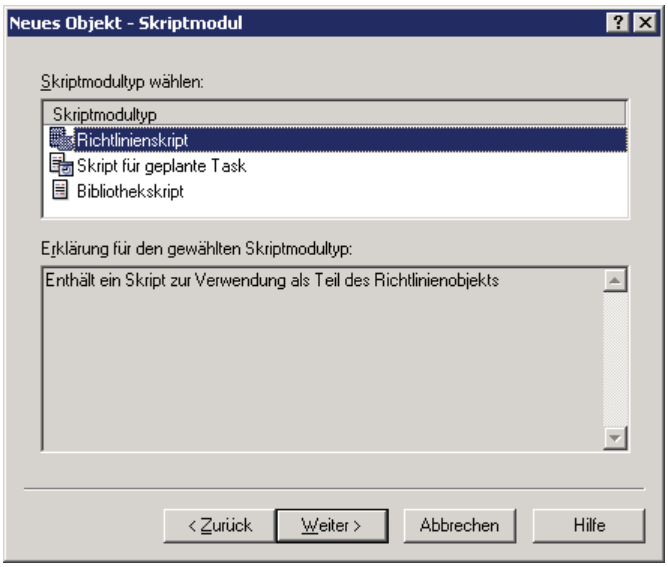
Um ein neues Skriptmodul zu erstellen, klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Script Modules** und wählen Sie **Neu | Skriptmodul**. Dann wird der Assistent „Neues Objekt – Skriptmodul" geöffnet.

Sie sollten benutzerdefinierte Skriptmodule in einem separaten Container speichern. Sie können wie folgt einen Container erstellen: Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Script Modules** und wählen Sie **Neu | Skriptcontainer**. Nachdem Sie einen Container erstellt haben, können Sie mit Hilfe des Assistenten ein Skriptmodul zu dem Container anstatt direkt zu den **Script Modules** hinzufügen: Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Container und wählen Sie **Neu | Skriptmodul** aus.

Die erste Seite des Assistenten entspricht der folgenden Abbildung.



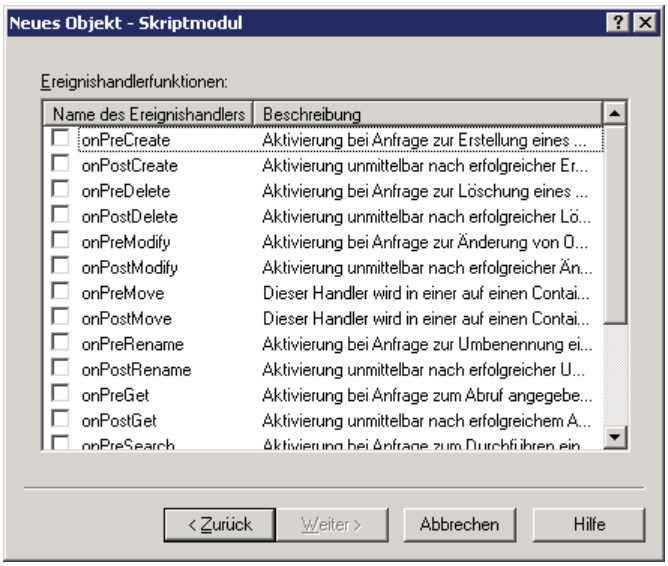
Geben Sie einen Namen und eine Beschreibung für das neue Skriptmodul ein und wählen Sie die Skriptsprache aus. Klicken Sie dann auf **Weiter**. Die nächste Seite sollte der folgenden Abbildung entsprechen.



Wählen Sie auf dieser Seite einen Skriptmodultyp aus. Wählen Sie **Richtlinienskript** aus, um ein Skript zu erstellen, das als Teil des Richtlinienobjekts verwendet werden soll. Die anderen Optionen lauten:

- **Skript für geplante Task.** Ein Skript, für das Sie die Ausführung für den Verwaltungsdienst planen können.
- **Bibliothekskript.** Ein Skript, das von anderen Skriptmodulen verwendet werden soll. Sie können häufig verwendete Funktionen in einem eigenständigen Skriptmodul sammeln und es in andere Module einschließen, die diese Funktionen benötigen. So können Sie Teile vorhandener Skripts wieder verwenden und somit Aufwand und Zeit für die Entwicklung reduzieren.

Wählen Sie **Richtlinienskript** aus und klicken Sie dann auf **Weiter**. Nun wird die in der folgenden Abbildung gezeigte Seite mit einer Liste von Ereignishandlerfunktionen angezeigt.



Wählen Sie auf dieser Seite Funktionen aus, die in dem Skript verwendet werden sollen, und klicken Sie dann auf **Weiter**. Klicken Sie dann auf **Fertig stellen**, um das Skriptmodul zu erstellen.

Anweisungen und Richtlinien für das Entwickeln von Richtlinienskripts finden Sie im Quest One ActiveRoles Software Development Kit (SDK).

Auf der Quest One ActiveRoles-Konsole können Sie importierte sowie neu erstellte Skripts anzeigen und ändern.

Bearbeiten eines Skripts

Um ein Skript zu bearbeiten, wählen Sie es in der Konsolenstruktur unter **Configuration/Script Modules** aus. Sie können das Skript im Bereich „Details" anzeigen und ändern. Um die Bearbeitung des Skripts zu beginnen, klicken Sie mit der rechten Maustaste auf das Skriptmodul und klicken Sie dann auf **Skript bearbeiten**. Klicken Sie dann auf **Ja**, um den Vorgang zu bestätigen. Sie können das Skript im Bereich „Details" ändern.

Wenn Sie das Skript bearbeiten, wird in der Konsolenstruktur neben dem Namen des Skriptmoduls ein rotes Sternchen angezeigt. Dies zeigt an, dass die am Skript vorgenommen Änderungen noch nicht gespeichert wurden. Sie können die Änderungen wie folgt rückgängig machen oder speichern:

- Drücken Sie zum Rückgängigmachen von Änderungen STRG+Z. (Sie können rückgängig gemacht Änderungen auch wiederherstellen: Drücken Sie STRG+Y).
- Um alle nicht gespeicherten Änderungen rückgängig zu machen, klicken Sie mit der rechten Maustaste auf das Skriptmodul und klicken Sie dann auf **Änderungen verwerfen**. (Dieser Vorgang ist nicht umkehrbar: Wenn Sie diesen Befehl ausführen, gehen Ihre Änderungen an dem Skript verloren).
- Um die Änderungen zu speichern, klicken Sie mit der rechten Maustaste auf das Skriptmodul und klicken Sie dann auf **Skript auf Server speichern**.

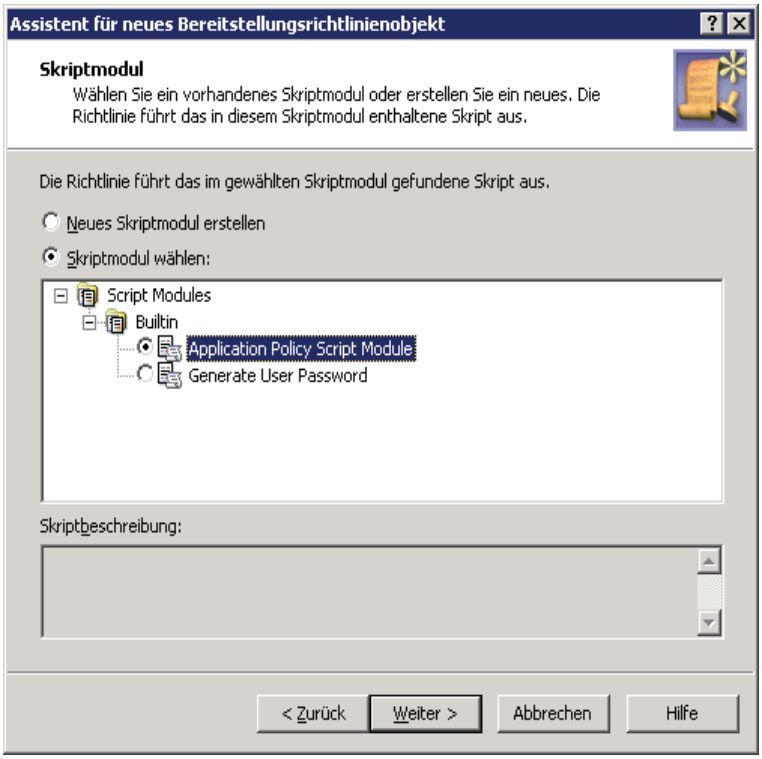
Wenn das Skriptmodul bereit ist, können Sie eine Skriptrichtlinie konfigurieren, die das vorbereitete Skriptmodul verwendet.

Mit Quest One ActiveRoles können Sie einen Debugger an den Skripthost des Verwaltungsdienstes für ein bestimmtes Richtlinienskript oder geplantes Taskskript anfügen. Wenn das Skript von dem angegebenen Verwaltungsdienst ausgeführt wird, kann der Debugger ggf. beim Identifizieren und Isolieren von Problemen mit der Richtlinie oder dem Task helfen, die bzw. der auf diesem Skript basiert.

Um das Debuggen eines Skripts auf der Quest One ActiveRoles-Konsole zu aktivieren, zeigen Sie das Dialogfeld **Eigenschaften** für das Skriptmodul an, das das Skript enthält, öffnen Sie die Registerkarte **Fehlerbehebung** und aktivieren Sie das Kontrollkästchen **Debuggen aktivieren**. Wählen Sie in der Liste **Debug auf Server** den Verwaltungsdienst aus, für den der Debugger ausgeführt werden soll.

Konfigurieren einer Richtlinie zur Ausführung eines Skripts

Um eine skriptbasierte Richtlinie zu konfigurieren, wählen Sie **Skriptausführung** auf der Seite **Richtlinientyp auswählen** im Assistenten für neues Bereitstellungsrichtlinienobjekt oder im Assistenten „Neues Deprovisionsrichtlinienobjekt" oder im Assistenten „Richtlinie hinzufügen" aus. Klicken Sie dann auf **Weiter**, damit die Seite **Skriptmodul** angezeigt wird.


Assistent für neues Bereitstellungsrichtlinienobjekt
Skriptmodul
Wählen Sie ein vorhandenes Skriptmodul oder erstellen Sie ein neues. Die Richtlinie führt das in diesem Skriptmodul enthaltene Skript aus.
Die Richtlinie führt das im gewählten Skriptmodul gefundene Skript aus.
Neues Skriptmodul erstellen
Skriptmodul wählen:
Script Modules
Builtin
Application Policy Script Module
Generate User Password
Skriptbeschreibung:
< Zurück
Weiter >
Abbrechen
Hilfe

Klicken Sie auf dieser Seite auf **Skriptmodul wählen** und wählen Sie das Skriptmodul aus. Klicken Sie dann auf **Weiter** und befolgen Sie die Anweisungen im Assistenten, um das Richtlinienobjekt zu erstellen.

Verfahren zum Konfigurieren einer Skriptausführungsrichtlinie

Gehen Sie folgendermaßen vor, um eine Richtlinie zur Skriptausführung zu konfigurieren:

1. Wählen Sie auf der Seite **Zu konfigurierende Richtlinie** die Option **Skriptausführung** aus und klicken Sie dann auf **Weiter**.
2. Führen Sie auf der Seite **Skriptmodul** eine der folgenden Operationen aus:
   - Um ein vorhandenes Skriptmodul zu verwenden, klicken Sie auf **Skriptmodul** wählen und wählen Sie dann das Skriptmodul im Feld unter dieser Option aus.
   - Um ein neues Skriptmodul zu erstellen, klicken Sie auf **Neues Skriptmodul erstellen** und klicken Sie dann auf **Weiter**. Geben Sie dann einen Namen für das Skriptmodul ein und klicken Sie anschließend auf **Weiter**. Wählen Sie dann den Ereignishandler aus, der im Skriptmodul enthalten sein soll.
3. Klicken Sie auf **Weiter**.
4. Gehen Sie auf der Seite **Richtlinienparameter** folgendermaßen vor:
   a) Wählen Sie erforderlichenfalls aus der Liste **Funktion zur Deklaration von Parametern** die Funktion aus, die die für diese Richtlinie spezifischen Parameter definiert.

      *Die Liste enthält die Namen aller im ausgewählten Skriptmodul gefundenen Skriptfunktionen. Die Richtlinie verfügt über die Parameter, die von der Funktion definiert sind, die im Feld **Funktion zur Deklaration von Parametern** angegeben ist. Normalerweise ist dies eine Funktion mit der Bezeichnung „onInit".*

   b) Zeigen Sie unter **Parameterwerte** die Werte der Richtlinienparameter an oder ändern Sie sie. Um den Wert eines Parameters zu ändern, wählen Sie den Namen des Parameters aus und klicken Sie dann auf **Bearbeiten**.

      *Durch Anklicken von **Bearbeiten** wird eine Seite angezeigt, auf der Sie einen oder mehrere Werte für den ausgewählten Parameter hinzufügen, entfernen oder auswählen können. Für jeden Parameter definiert die Funktion, die für die Deklaration von Parametern verwendet wird, den Namen des Parameters und andere Merkmale wie etwa eine Beschreibung, eine Liste der möglichen Werte, den Standardwert und ob ein Wert erforderlich ist oder nicht. Wenn eine Liste der möglichen Werte definiert ist, dann können Sie nur Werte aus dieser Liste auswählen.*
5. Auf der Seite **Richtlinie erzwingen** können Sie Objekte angeben, auf die dieses Richtlinienobjekt angewandt werden soll:
   - Klicken Sie auf **Hinzufügen** und verwenden Sie das Objekt **Objekte auswählen**, um die gewünschten Objekte auszuwählen.
6. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Gehen Sie folgendermaßen vor, um ein Skriptmodul zu erstellen:

1. Wählen Sie in der Konsolenstruktur unter **Configuration | Script Modules** den Ordner aus, zu dem Sie das Skriptmodul hinzufügen möchten.

   *Gehen Sie folgendermaßen vor, um einen neuen Ordner zu erstellen: Klicken Sie mit der rechten Maustaste auf **Script Modules** und wählen Sie dann **Neu | Skriptcontainer**. Auf die gleiche Weise können Sie einen Unterordner in einem Ordner erstellen: Klicken Sie mit der rechten Maustaste auf den Ordner und wählen Sie **Neu | Skriptcontainer** aus.*
2. Klicken Sie mit der rechten Maustaste auf den Ordner und wählen Sie **Neu | Skriptmodul** aus.
3. Geben Sie Namen und die Sprache des zu erstellenden Moduls an. Klicken Sie dann auf **Weiter**.
4. Klicken Sie unter **Skriptmodultyp wählen** auf den Typ des zu erstellenden Moduls. Klicken Sie dann auf **Weiter**.

5. Wenn Sie den Typ **Richtlinienskript** für das Modul ausgewählt haben, wählen Sie die Ereignishandler aus, die das Modul enthalten soll, und klicken Sie dann auf **Weiter**.
6. Klicken Sie auf **Fertig stellen**.

Gehen Sie folgendermaßen vor, um ein Skriptmodul zu bearbeiten:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Script Modules**.
2. Klicken Sie unter **Script Modules** auf den Ordner mit dem Skriptmodul, das Sie bearbeiten möchten.
3. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf das Skriptmodul und klicken Sie dann auf **Skript bearbeiten**.
4. Verwenden Sie den Bereich „Details", um Änderungen am Skript vorzunehmen.
5. Klicken Sie mit der rechten Maustaste auf das Skriptmodul in der Konsolenstruktur und führen Sie dann einen der folgenden Vorgänge durch:
   - Um die vorgenommenen Änderungen zu senden, klicken Sie auf **Skript auf Server speichern**.
   - Um den Skript-Editor ohne Speicherung der Änderungen zu beenden, klicken Sie auf **Änderungen verwerfen**.

Gehen Sie folgendermaßen vor, um ein Skriptmodul zu importieren:

1. Wählen Sie in der Konsolenstruktur unter **Configuration | Script Modules** den Ordner aus, zu dem Sie das Skriptmodul hinzufügen möchten.

   *Gehen Sie folgendermaßen vor, um einen neuen Ordner zu erstellen: Klicken Sie mit der rechten Maustaste auf **Script Modules** und wählen Sie dann **Neu | Skriptcontainer**. Auf die gleiche Weise können Sie einen Unterordner in einem Ordner erstellen: Klicken Sie mit der rechten Maustaste auf den Ordner und wählen Sie **Neu | Skriptcontainer** aus.*
2. Klicken Sie mit der rechten Maustaste auf den Ordner und klicken Sie dann auf **Importieren**.
3. Wählen Sie die Datei aus, die das zu importierende Skript enthält, und klicken Sie dann auf **Öffnen**.

Gehen Sie folgendermaßen vor, um ein Skriptmodul zu exportieren:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Script Modules**.
2. Wählen Sie unter **Script Modules** den Ordner mit dem Skriptmodul aus, das Sie exportieren möchten.
3. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf das Skriptmodul und wählen Sie dann **Alle Aufgaben | Exportieren**.
4. Geben Sie die Datei an, in der Sie das Skript speichern möchten, und klicken Sie dann auf **Speichern**.

Szenario: Einschränken des Gruppenbereichs

In diesem Szenario wird die Konfiguration einer Richtlinie beschrieben, die die Erstellung von universellen Gruppen verhindert. Mit dieser Richtlinie verhindert die Quest One ActiveRoles-Konsole oder das Web-Interface, dass ein Administrator eine neue universelle Gruppe erstellt oder eine vorhandene Gruppe in eine universelle Gruppe umwandelt.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Bereiten Sie das Skript vor, mit dem dieses Szenario implementiert wird.
2. Erstellen und konfigurieren Sie das Richtlinienobjekt für die Ausführung dieses Skripts.
3. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Folglich kann die Quest One ActiveRoles-Konsole oder das Web-Interface nicht zur Festlegen der Option „Bereich der universellen Gruppe" beim Erstellen einer neuen Gruppe oder beim Ändern einer vorhandenen Gruppe in dem Container verwendet werden, den Sie in Schritt 3 ausgewählt haben. Wenn Sie beispielsweise die Option **Universell** unter **Gruppenbereich** auswählen und dann im Assistenten „Neues Objekt - Gruppe" auf **Weiter** klicken, zeigt die Quest One ActiveRoles-Konsole eine Fehlermeldung an, die angibt, dass die Erstellung einer universellen Gruppe unzulässig ist.

In den folgenden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Vorbereiten des Skriptmoduls

Das in diesem Szenario verwendete Skript wird mit dem Quest One ActiveRoles SDK installiert. Standardmäßig lauten der Pfad und Name der Skriptdatei wie folgt: "%ProgramFiles%\Quest Software\Quest One ActiveRoles\SDK\Samples\RestrictGroupScope\RestrictGroupScope.ps1"

Das Skript übernimmt bei Erhalt einer an den Administrationsdienst gesendeten Anfrage zur Überprüfung der Eigenschaftswerte die Kontrolle und analysiert den Wert des Attributs „groupType", um zu ermitteln, ob versucht wurde, die Option „Bereich der universellen Gruppe" zu aktivieren. Wenn das Skript erkennt, dass der angenommene Wert „groupType" dazu führen würde, dass eine Gruppe als eine universelle Gruppe konfiguriert wird, generiert es ein Richtlinienverletzungsereignis im Verwaltungsdiensts. Daraufhin zeigt die Anwendung, die die Anfrage initiiert hat (wie etwa die Quest One ActiveRoles-Konsole oder das Web-Interface) eine vom Skript bereitgestellte Fehlermeldung. Weitere Informationen finden Sie unter „Einschränken des Gruppenbereichs" in der Quest One ActiveRoles SDK-Dokumentation.

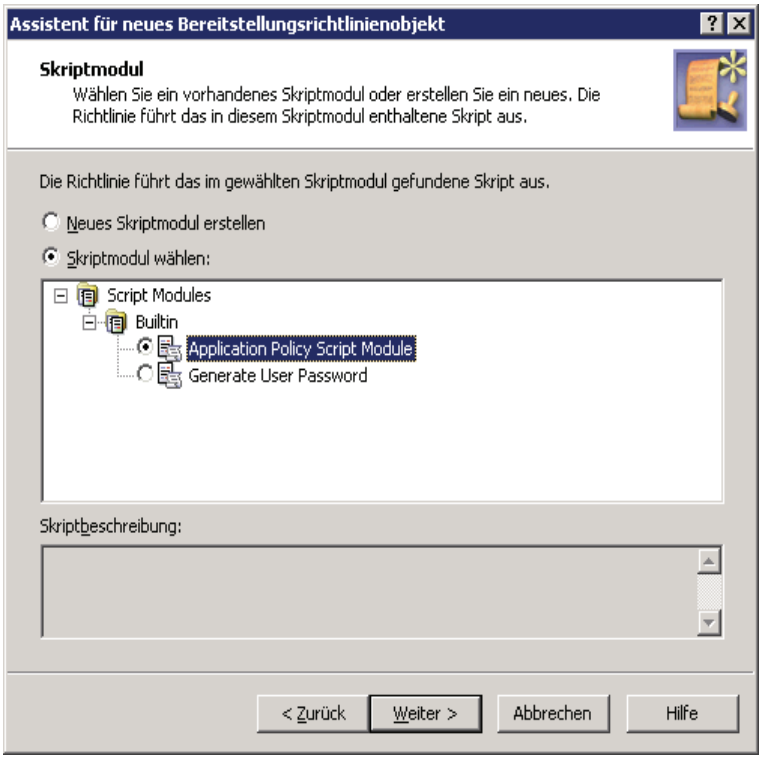
Um das Skript zu importieren, klicken Sie mit der rechten Maustaste auf den Container **Script Modules** in der Quest One ActiveRoles-Konsole und klicken Sie dann auf **Importieren**. Wählen Sie dann die Datei **RestrictGroupScope.ps1** aus und öffnen Sie sie.

Schritt 2: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten für neues Bereitstellungsrichtlinienobjekt erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter Erstellen eines Richtlinienobjekts im Abschnitt Verwaltungsaufgaben für Richtlinienobjekte weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Zu konfigurierende Richtlinie** des Assistenten auf **Skriptausführung**. Klicken Sie dann auf **Weiter**.

Klicken Sie auf der Seite **Skriptmodul** auf **Skriptmodul wählen** und wählen Sie in der Liste der Skriptmodule den Eintrag **RestrictGroupScope** aus, wie in der folgenden Abbildung gezeigt.


Assistent für neues Bereitstellungsrichtlinienobjekt
Skriptmodul
Wählen Sie ein vorhandenes Skriptmodul oder erstellen Sie ein neues. Die Richtlinie führt das in diesem Skriptmodul enthaltene Skript aus.
Die Richtlinie führt das im gewählten Skriptmodul gefundene Skript aus.
Neues Skriptmodul erstellen
Skriptmodul wählen:
Script Modules
Builtin
Application Policy Script Module
Generate User Password
Skriptbeschreibung:
< Zurück
Weiter >
Abbrechen
Hilfe

Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 3: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten für neues Bereitstellungsrichtlinienobjekt anwenden, oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen bezüglich der Anwendung eines Richtlinienobjekts finden Sie unter Anwenden von Richtlinienobjekten und Verwalten des Richtlinienbereichs weiter oben in diesem Kapitel.

Benutzerkonto-Deprovisionierung

Richtlinien dieser Kategorie dienen zum Automatisieren der folgenden Aufgaben im Zusammenhang mit der Deprovisionierung von Benutzerkonten:

- Benutzerkonto deaktivieren
- Festlegen des Benutzerkennworts auf einen zufälligen Wert
- Festlegen der Anmeldenamen des Benutzers auf zufällige Werte
- Benutzerkonto umbenennen
- Ändern anderer Eigenschaften des Benutzerkontos

Wenn Sie eine Richtlinie dieser Kategorie konfigurieren, geben Sie an, wie Quest One ActiveRoles bei einer Deprovisionsanforderung für einen Benutzer das Konto des Benutzers in Active Directory ändern soll. Der Deprovisionierungsvorgang muss dazu führen, dass der Benutzer sich nicht mehr am Netzwerk anmelden kann.

Sie können auch eine Richtlinie so konfigurieren, dass sie beliebige Benutzereigenschaften aktualisiert, z.B., die, die die Mitgliedschaft von Benutzern in verwalteten Einheiten von Quest One ActiveRoles regulieren. So kann die Richtlinie das Hinzufügen oder Entfernen von Benutzern, für die die Bereitstellung zurückgenommen wird, aus verwalteten Einheiten automatisieren.

Funktionsweise dieser Richtlinie

Beim Verarbeiten einer Deprovisionsanforderung für einen Benutzer verwendet Quest One ActiveRoles diese Richtlinie, um das Konto des Benutzers so zu ändern, dass dieser Benutzer sich nicht mehr am Netzwerk anmelden kann.

Es kann auch eine Richtlinie zum Aktualisieren von Benutzerkonten konfiguriert werden. Abhängig von der Richtlinienkonfiguration hat jede richtlinienbasierte Aktualisierung folgende Ergebnisse:

- Bestimmte Teile von Kontoinformationen werden aus dem Verzeichnis entfernt, indem bestimmte Eigenschaften auf „leere" Werte zurückgesetzt werden.
- Bestimmte Eigenschaften von Benutzerkonten werden auf neue, nicht leere Werte zurückgesetzt.

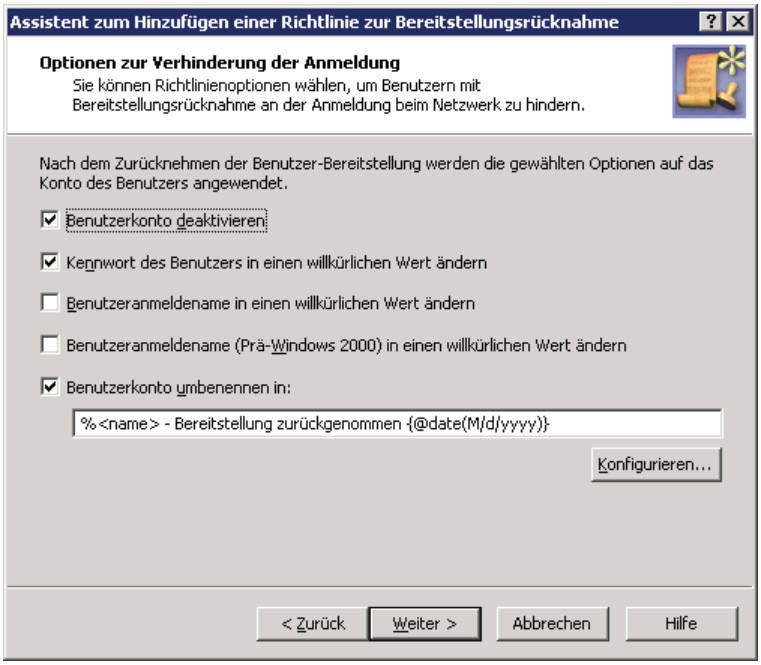
Eine Richtlinie kann so konfiguriert werden, dass sie folgende neue Eigenschaftswerte einschließt:

- Eigenschaften des Benutzerkontos, für das die Bereitstellung zurückgenommen wird. Diese Eigenschaften wurden vor dem Beginn des Rücknahmevorgangs für den Benutzer aus dem Verzeichnis abgerufen
- Eigenschaften des Benutzers, der die Anfrage zur Deprovisionierung gestellt hat
- Datum und Uhrzeit der Deprovisionierung für den Benutzer

Quest One ActiveRoles ändert also bei der Deprovisionierung für einen Benutzer das Benutzerkonto in Active Directory so, wie es von der gültigen Richtlinie „Benutzerkontodeprovisionierung" bestimmt wird.

Konfigurieren der Richtlinie „Benutzerkontodeprovisionierung“

Um eine Benutzerkonto-Deprovisionierungsrichtlinie zu konfigurieren, wählen Sie **Benutzerkonto-Deprovisionierung** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten „Neues Deprovisionsrichtlinienobjekt“ oder im Assistenten „Deprovisionsrichtlinie hinzufügen“ aus. Klicken Sie dann auf **Weiter**, damit die Seite **Optionen zur Verhinderung der Anmeldung** angezeigt wird.


Assistent zum Hinzufügen einer Richtlinie zur Bereitstellungsrücknahme
Optionen zur Verhinderung der Anmeldung
Sie können Richtlinienoptionen wählen, um Benutzern mit Bereitstellungsrücknahme an der Anmeldung beim Netzwerk zu hindern.
Nach dem Zurücknehmen der Benutzer-Bereitstellung werden die gewählten Optionen auf das Konto des Benutzers angewendet.
Benutzerkonto deaktivieren
Kennwort des Benutzers in einen willkürlichen Wert ändern
Benutzeranmeldename in einen willkürlichen Wert ändern
Benutzeranmeldename (Prä-Windows 2000) in einen willkürlichen Wert ändern
Benutzerkonto umbenennen in:
%<name> - Bereitstellung zurückgenommen {@date(M/d/yyyy)}
Konfigurieren...
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite können Sie Optionen auswählen, die Anmeldungen mit diesem Konto verhindern. Die Optionsnamen sind selbsterklärend:

- Benutzerkonto deaktivieren
- Kennwort des Benutzers in einen willkürlichen Wert ändern
- Benutzeranmeldename in einen willkürlichen Wert ändern
- Benutzeranmeldename (Prä-Windows 2000) in einen willkürlichen Wert ändern

Aktivieren Sie die Kontrollkästchen neben den Optionen, die die Richtlinie anwenden soll.

Durch Aktivieren des Kontrollkästchens **Benutzerkonto umbenennen** in weisen Sie die Richtlinie an, den Benutzernamen des Kontos zu ändern. Mit dieser Option können Sie eine *Eigenschaftsaktualisierungsregel* konfigurieren, die angibt, wie der Benutzername geändert werden soll. Im folgenden Unterabschnitt werden Anweisungen zum Konfigurieren einer Eigenschaftsaktualisierungsregel bereitgestellt.

Dabei wird der Benutzername als Beispiel verwendet.

Konfigurieren einer Eigenschaftsaktualisierungsregel Um eine Eigenschaftsaktualisierungsregel für den Benutzernamen zu konfigurieren, klicken Sie auf die Schaltfläche **Konfigurieren**. Daraufhin wird das Dialogfeld **Wert konfigurieren** angezeigt, das weiter oben in diesem Kapitel beschrieben ist (siehe Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften“). In diesem Dialogfeld können Sie einen Wert für die Bedingung **’Name’ muss sein** konfigurieren, ähnlich wie beim Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften“.

Um mit dem Konfigurieren eines Wertes zu beginnen, klicken Sie im Dialogfeld **Hinzufügen** auf **Wert konfigurieren**. Daraufhin wird das Fenster **Eintrag hinzufügen** angezeigt:

Ein Wert entsteht durch Verkettung von mindestens einem Eintrag. Im Fenster **Eintrag hinzufügen** können Sie den Typ des hinzuzufügenden Eintrags auswählen und den Eintrag dann konfigurieren. In der folgenden Tabelle werden die verfügbaren Eintragstypen zusammengefasst.

EINTRAGSTYP	BESCHREIBUNG
Text	Fügt dem Wert eine Textzeichenfolge hinzu.
Benutzereigenschaft	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) des Benutzerkontos hinzu, für das die Bereitstellung zurückgenommen wird.
Eigenschaft der übergeordneten Organisationseinheit	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) einer Organisationseinheit in der Containerhierarchie über dem Benutzerkonto hinzu, für das die Bereitstellung zurückgenommen wird.
Eigenschaft der übergeordneten Domäne	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) der Domäne des Benutzerkontos hinzu, für das die Bereitstellung zurückgenommen wird.
Datum und Uhrzeit	Fügt das Datum und die Uhrzeit der Deprovisionierung des Kontos hinzu.
Initiator-ID	Fügt eine Zeichenfolge hinzu, die den Initiator identifiziert, d.h. den Benutzer, der die Rücknahmeanforderung gestellt hat. Dieser Eintrag besteht aus Eigenschaften, die im Zusammenhang mit dem Initiator stehen und die aus dem Verzeichnis abgerufen wurden.

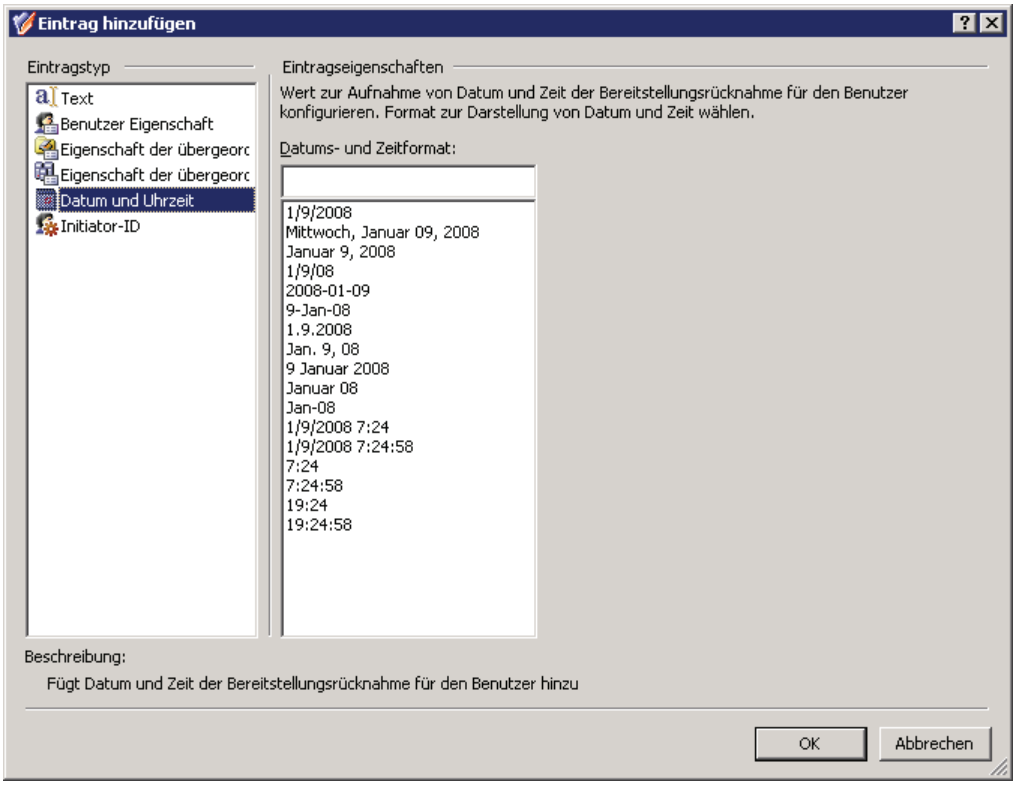
Die Anweisungen zum Konfigurieren eines Eintrags hängen vom Eintragstyp ab. Sie können die im Abschnitt Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften“ weiter oben in diesem Kapitel beschriebenen Anweisungen befolgen, um einen Eintrag eines der folgenden Typen zu konfigurieren:

- **Text.** Siehe Unterabschnitt Eintragstyp: Text.
- **Benutzereigenschaft.** Siehe Unterabschnitt Eintragstyp: <Objekt>eigenschaft.
- **Eigenschaft der übergeordneten Organisationseinheit.** Siehe Unterabschnitt Eintragstyp: Eigenschaft der übergeordneten Organisationseinheit.
- **Eigenschaft der übergeordneten Domäne.** Siehe Unterabschnitt Eintragstyp: Eigenschaft der übergeordneten Domäne.

In den folgenden Unterabschnitten werden die Einträge **Datum und Uhrzeit** und **Initiator-ID** erörtert.

Eintragstyp: Datum und Uhrzeit

Wenn Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** den Typ **Datum und Uhrzeit** auswählen, ähnelt der Bereich **Eintragseigenschaften** der folgenden Abbildung.

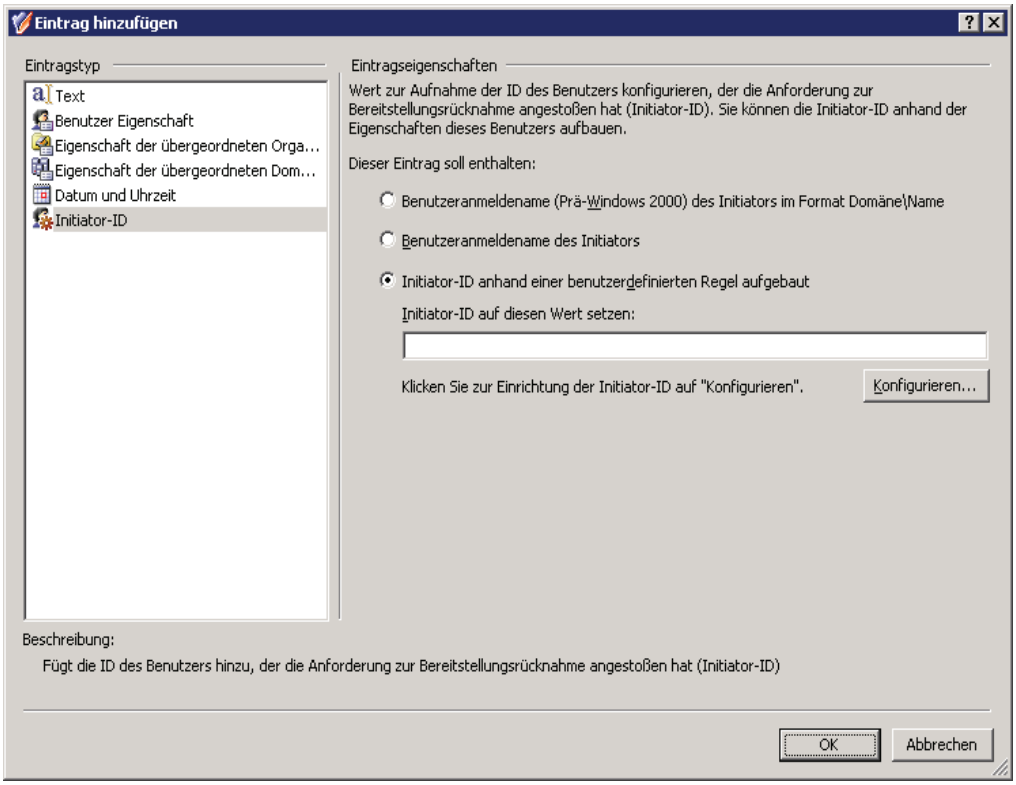


Durch die Verwendung dieses Eintragstyps können Sie einen Eintrag hinzufügen, der das Datum und die Uhrzeit der Deprovisionierung für das Benutzerkonto darstellt.

Klicken Sie in der Liste unter **Datums- und Zeitformat** auf das gewünschte Datums- oder Uhrzeitformat. Klicken Sie dann auf **OK**, um das Fenster **Eintrag hinzufügen** zu schließen.

Eintragstyp: Initiator-ID

Wenn Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** den Typ **Initiator-ID** auswählen, ähnelt der Bereich **Eintragseigenschaften** der folgenden Abbildung.


Eintrag hinzufügen
Eintragstyp
Text
Benutzer Eigenschaft
Eigenschaft der übergeordneten Orga...
Eigenschaft der übergeordneten Dom...
Datum und Uhrzeit
Initiator-ID
Eintragseigenschaften
Wert zur Aufnahme der ID des Benutzers konfigurieren, der die Anforderung zur Bereitstellungsrücknahme angestoßen hat (Initiator-ID). Sie können die Initiator-ID anhand der Eigenschaften dieses Benutzers aufbauen.
Dieser Eintrag soll enthalten:
Benutzeranmeldename (Prä-Windows 2000) des Initiators im Format Domäne\Name
Benutzeranmeldename des Initiators
Initiator-ID anhand einer benutzerdefinierten Regel aufgebaut
Initiator-ID auf diesen Wert setzen:
Klicken Sie zur Einrichtung der Initiator-ID auf "Konfigurieren".
Konfigurieren...
Beschreibung:
Fügt die ID des Benutzers hinzu, der die Anforderung zur Bereitstellungsrücknahme angestoßen hat (Initiator-ID)
OK
Abbrechen

Mit diesem Eintragstyp können Sie eine Zeichenfolge hinzufügen, die den Initiator identifiziert, d.h. den Benutzer, der die Rücknahmeanforderung gestellt hat. Die Richtlinie generiert die Initiator-ID anhand bestimmter Kontoeigenschaften des Initiators, z.B. anhand des Benutzer-Anmeldenamens. Zum Verwenden anderer Eigenschaften kann eine benutzerdefinierte Regel konfiguriert werden.

Sie können eine vorkonfigurierte Regel auswählen oder eine benutzerdefinierte Regel konfigurieren, um die Initiator-ID zu generieren. Die vorkonfigurierten Regeln ermöglichen Ihnen, die Initiator-ID auf einen der folgenden Werte zu setzen:

- Den Benutzer-Anmeldenamen (Prä-Windows 2000) des Initiators in der Form *Domänenname**Benutzername*
- Den Benutzer-Anmeldenamen des Initiators

Mit einer benutzerdefinierten Regel können Sie die Initiator-ID aus anderen auf den Initiator bezogenen Eigenschaften zusammensetzen.

Konfigurieren einer benutzerdefinierten Regel zum Erstellen der Initiator-ID

Klicken Sie zum Konfigurieren einer benutzerdefinierten Regel für die Initiator-ID auf die unterste Option unter **Eintragseigenschaften** und klicken Sie dann auf die Schaltfläche **Konfigurieren**. Daraufhin wird das Dialogfeld **Wert konfigurieren** angezeigt, das weiter oben in diesem Kapitel beschrieben ist (siehe Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften"). In diesem Dialogfeld können Sie einen Wert für die Bedingung **„Initiator-ID" muss sein** konfigurieren, ähnlich wie beim Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften".

Um mit dem Konfigurieren eines Wertes zu beginnen, klicken Sie im Dialogfeld **Hinzufügen** auf **Wert konfigurieren**. Daraufhin wird das Fenster **Eintrag hinzufügen** angezeigt:

Ein Wert entsteht durch Verkettung von mindestens einem Eintrag. Im Fenster **Eintrag hinzufügen** können Sie den Typ des hinzuzufügenden Eintrags auswählen und den Eintrag dann konfigurieren. In der folgenden Tabelle werden die verfügbaren Eintragstypen zusammengefasst.

EINTRAGSTYP	BESCHREIBUNG
Text	Fügt dem Wert eine Textzeichenfolge hinzu.
Eigenschaft des Initiators	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) des Benutzerkontos des Initiators hinzu.
Eigenschaft der übergeordneten Organisationseinheit	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) einer Organisationseinheit in der Containerhierarchie über dem Benutzerkonto des Initiators hinzu.
Eigenschaft der übergeordneten Domäne	Fügt eine ausgewählte Eigenschaft (oder einen Teil einer Eigenschaft) der Domäne des Benutzerkontos des Initiators hinzu.

Die Anweisungen zum Konfigurieren eines Eintrags hängen vom Eintragstyp ab. Sie finden Anweisungen für jeden Eintragstyp im Abschnitt Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften" weiter oben in diesem Kapitel.

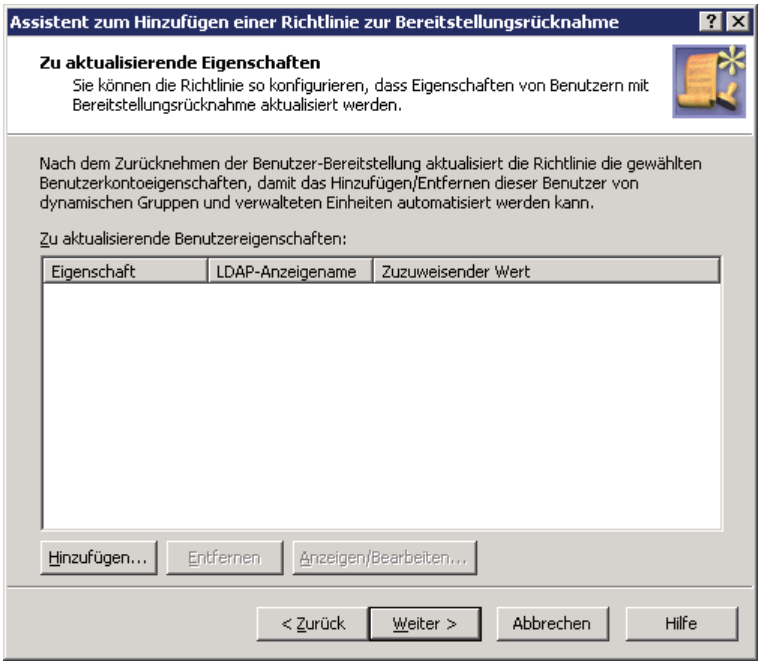
- **Text.** Siehe Unterabschnitt Eintragstyp: Text.
- **Eigenschaft des Initiators.** Siehe Unterabschnitt Eintragstyp: <Objekt>eigenschaft.
- **Eigenschaft der übergeordneten Organisationseinheit.** Siehe Unterabschnitt Eintragstyp: Eigenschaft der übergeordneten Organisationseinheit.
- **Eigenschaft der übergeordneten Domäne.** Siehe Unterabschnitt Eintragstyp: Eigenschaft der übergeordneten Domäne.

Klicken Sie nach dem Konfigurieren eines Wertes für die Bedingung **'Initiator-ID' muss sein** auf **OK**, um das Dialogfeld **Wert konfigurieren** zu schließen. Damit wird der Wert den Eintragseigenschaften für die Initiator-ID hinzugefügt. Nötigenfalls können Sie den Wert ändern. Klicken Sie dazu im Fenster **Eintrag hinzufügen** auf die Schaltfläche **Konfigurieren**, und verwalten Sie dann im Dialogfeld **Wert konfigurieren** die Liste der Einträge.

Klicken Sie nach dem Konfigurieren des Eintrags **Initiator-ID** auf **OK**, um das Fenster **Eintrag hinzufügen** zu schließen. Der Eintrag wird dem Dialogfeld **Wert konfigurieren** für die Bedingung **'Name' muss sein** hinzugefügt.

Klicken Sie nach dem Konfigurieren eines Wertes für die Bedingung **'Name' muss sein** auf **OK** um das Dialogfeld **Wert konfigurieren** zu schließen. Nun wird die Regel der Seite **Optionen zur Verhinderung der Anmeldung** des Assistenten hinzugefügt. Nötigenfalls können Sie die Regel ändern. Klicken Sie dazu auf die Schaltfläche **Konfigurieren** und verwalten Sie dann die Liste der Einträge im Dialogfeld **Wert konfigurieren**.

Wenn Sie die Seite **Optionen zur Verhinderung der Anmeldung** abgeschlossen haben, klicken Sie auf **Weiter**, um die Seite **Zu aktualisierende Eigenschaften** anzuzeigen:


Assistent zum Hinzufügen einer Richtlinie zur Bereitstellungsrücknahme
Zu aktualisierende Eigenschaften
Sie können die Richtlinie so konfigurieren, dass Eigenschaften von Benutzern mit Bereitstellungsrücknahme aktualisiert werden.
Nach dem Zurücknehmen der Benutzer-Bereitstellung aktualisiert die Richtlinie die gewählten Benutzerkontoeigenschaften, damit das Hinzufügen/Entfernen dieser Benutzer von dynamischen Gruppen und verwalteten Einheiten automatisiert werden kann.
Zu aktualisierende Benutzereigenschaften:
Eigenschaft
LDAP-Anzeigename
Zuzuweisender Wert
Hinzufügen...
Entfernen
Anzeigen/Bearbeiten...
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite können Sie eine Liste von Benutzereigenschaften einrichten, die die Richtlinie aktualisieren soll. Jeder Eintrag in der Liste schließt die folgenden Informationen ein:

- **Eigenschaft.** Bei der Deprovisionierung für einen Benutzer aktualisiert Quest One ActiveRoles diese Eigenschaft des Benutzerkontos.
- **LDAP-Anzeigename.** Identifiziert die zu aktualisierende Eigenschaft eindeutig.
- **Zuzuweisender Wert.** Nach dem Abschluss des Deprovisionierungsvorgangs besitzt die Eigenschaft den durch diese Syntax definierten Wert.

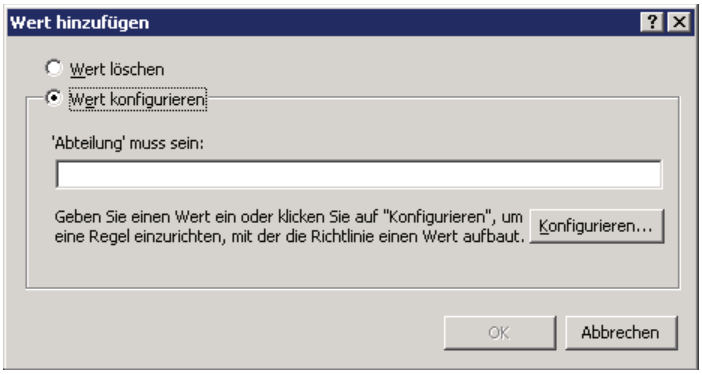
Sie können die Liste auf dieser Seite mit folgenden Schaltflächen verwalten:

- **Hinzufügen.** Ermöglicht das Auswählen einer Benutzereigenschaft und das Konfigurieren einer Aktualisierungsregel für diese Eigenschaft. Eine Eigenschaftsaktualisierungsregel gibt an, wie der neue Wert generiert werden soll, der der Eigenschaft zugewiesen wird.
- **Entfernen.** Wenn die Richtlinie eine bestimmte Eigenschaft nicht mehr aktualisieren soll, wählen Sie die Eigenschaft in der Liste aus und klicken Sie auf **Entfernen**.
- **Anzeigen/Bearbeiten.** Ermöglicht das Ändern der Aktualisierungsregel für die Eigenschaft, die Sie in der Liste auswählen.

Wenn Sie auf die Schaltfläche **Hinzufügen** klicken, wird das Dialogfeld **Objekteigenschaft wählen** angezeigt. In diesem können Sie Benutzereigenschaften auswählen, die die Richtlinie aktualisieren soll. Um eine Eigenschaft auszuwählen, aktivieren Sie das Kontrollkästchen neben dem Eigenschaftsnamen und klicken Sie dann auf **OK**.

Sie können mehrere Kontrollkästchen aktivieren. In diesem Fall werden die ausgewählten Eigenschaften der Liste auf der Seite des Assistenten hinzugefügt, und die Aktualisierungsregel wird so konfiguriert, dass sie diese Eigenschaften löscht, ihnen also den „leeren" Wert zuweist.

Wenn Sie eine einzelne Eigenschaft im Dialogfeld **Objekteigenschaft wählen** auswählen, wird das Dialogfeld **Wert hinzufügen** angezeigt, sodass Sie den Vorgang mit der Konfiguration einer Eigenschafts-Aktualisierungsregel fortsetzen können:


Wert hinzufügen
Wert löschen
Wert konfigurieren
'Abteilung' muss sein:
Geben Sie einen Wert ein oder klicken Sie auf "Konfigurieren", um eine Regel einzurichten, mit der die Richtlinie einen Wert aufbaut.
Konfigurieren...
OK
Abbrechen

Sie können eine der folgenden Aktualisierungsoptionen auswählen:

- **Wert löschen.** Veranlasst die Richtlinie dazu, der Eigenschaft den „leeren" Wert zuzuweisen.
- **Wert konfigurieren.** Ermöglicht das Konfigurieren eines Wertes für die Bedingung **'Eigenschaft' muss sein**.

Bei der zweiten Option müssen Sie einen Wert konfigurieren, den die Richtlinie bei der Deprovisionierung für einen Benutzer der Eigenschaft zuweisen soll. Sie können einen Wert auf die gleiche Weise konfigurieren wie beim Konfigurieren einer Eigenschaftsaktualisierungsregel für den Benutzernamen: Klicken Sie auf die Schaltfläche **Konfigurieren** und folgen Sie den Anweisungen weiter oben in diesem Abschnitt (siehe Dabei wird der Benutzername als Beispiel verwendet.).

Klicken Sie nach dem Konfigurieren eines Wertes auf **OK**, um das Dialogfeld **Wert hinzufügen** zu schließen. Der Eigenschaftsname wird zusammen mit der Eigenschaftsaktualisierungsregel der Seite des Assistenten hinzugefügt. Nötigenfalls können Sie die Aktualisierungsregel ändern, indem Sie unter der Eigenschaftenliste auf die Schaltfläche **Anzeigen/Bearbeiten** klicken. Dann wird ein Dialogfeld angezeigt, das dem Dialogfeld **Wert hinzufügen** ähnelt und in dem Sie eine andere Aktualisierungsoption auswählen oder einen anderen Wert für die Bedingung **'Eigenschaft' muss sein** festlegen können.

Klicken Sie nach dem Einrichten der Liste auf der Seite des Assistenten auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Verfahren zum Konfigurieren einer Benutzerkonto-Deprovisionierungsrichtlinie

So konfigurieren Sie eine Richtlinie zur Deprovisionierung für Benutzerkonten:

1. Wählen Sie auf der Seite **Zu konfigurierende Richtlinie** die Option **Benutzerkonto-Stilllegung** aus und klicken Sie dann auf **Weiter**.
2. Wählen Sie auf der Seite **Optionen zur Verhinderung der Anmeldung** die Optionen aus, die die Richtlinie anwenden soll, wenn Sie ein Benutzerkonto deprovisioniert. Sie können jede beliebige Kombination dieser Optionen auswählen, die Anmeldungen mit diesem Benutzerkonto verhindern.
   - Benutzerkonto deaktivieren
   - Kennwort des Benutzers in einen willkürlichen Wert ändern
   - Benutzeranmeldename in einen willkürlichen Wert ändern
   - Benutzeranmeldename (Prä-Windows 2000) in einen willkürlichen Wert ändern
   - Benutzerkonto umbenennen in
3. Wenn Sie **Benutzerkonto umbenennen in** ausgewählt haben, klicken Sie auf **Konfigurieren** und füllen Sie dann das Dialogfeld **Wert konfigurieren** aus, indem Sie das weiter unten in diesem Thema beschriebene Verfahren ausführen, um festzulegen, wie die Richtlinie den Benutzernamen bei der Deprovisionierung eines Benutzerkontos aktualisiert.
4. Klicken Sie auf **Weiter**.
5. Geben Sie auf der Seite **Zu aktualisierende Eigenschaften** an, wie die Richtlinie Benutzereigenschaften aktualisieren soll, wenn Sie ein Benutzerkonto deprovisioniert:
   - Klicken Sie auf **Hinzufügen** und füllen Sie dann das Dialogfeld **Objekteigenschaft wählen** aus, indem Sie das weiter unten in diesem Thema beschriebene Verfahren befolgen, um Eigenschafts-Aktualisierungsregeln hinzuzufügen.
   - Verwenden Sie **Ansicht/Bearbeiten**, um vorhandene Regeln zu ändern.
   - Verwenden Sie **Entfernen**, um vorhandene Regeln zu löschen.
6. Klicken Sie auf **Weiter**.
7. Auf der Seite **Richtlinie erzwingen** können Sie Objekte angeben, auf die dieses Richtlinienobjekt angewandt werden soll:
   - Klicken Sie auf **Hinzufügen** und verwenden Sie das Objekt **Objekte auswählen**, um die gewünschten Objekte auszuwählen.
8. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Gehen Sie folgendermaßen vor, um das Dialogfeld „Wert konfigurieren" abzuschließen:

1. Klicken Sie auf **Hinzufügen**.
2. Konfigurieren Sie einen Eintrag, in den der Wert aufgenommen werden soll (Anweisungen finden Sie unter Verfahren zum Konfigurieren von Einträgen).
3. Im Dialogfeld **Wert konfigurieren** fügen Sie Einträge hinzu, löschen oder bearbeiten vorhandene Einträge und klicken dann auf **OK**.

Gehen Sie folgendermaßen vor, um das Dialogfeld „Objekteigenschaft auswählen" abzuschließen:

1. Wählen Sie in der Liste **Objekteigenschaft** eine Objekteigenschaft aus und klicken Sie dann auf **OK**. Das Dialogfeld **Wert hinzufügen** wird angezeigt.

   *Wenn Sie mehrere Eigenschaften auswählen, wird das Dialogfeld **Wert hinzufügen** nicht angezeigt. Die Eigenschaften, die Sie ausgewählt haben, werden zur Liste auf der Seite **Zu aktualisierende Eigenschaften** hinzugefügt, und die Aktualisierungsregel wird so konfiguriert, dass sie diese Eigenschaften löscht, ihnen also den „leeren" Wert zuweist.*

2. Führen Sie im Dialogfeld **Wert hinzufügen** eine der folgenden Aktionen durch:
   - Wählen Sie **Wert löschen**, wenn die Aktualisierungsregel der Eigenschaft den Wert „leer" zuordnen soll.
   - Wählen Sie **Wert konfigurieren**, wenn die Aktualisierungsregel der Eigenschaft einen bestimmten, nicht leeren Wert zuordnen soll. Klicken Sie dann auf **Konfigurieren** und vervollständigen Sie das Dialogfeld **Wert konfigurieren** anhand der weiter oben in diesem Thema aufgeführten Verfahrensweise.

Szenario 1: Deaktivieren und Umbenennen von Benutzerkonten bei der Deprovisionierung für einen Benutzer

Die in diesem Szenario beschriebene Richtlinie führt während der Deprovisionierung für einen Benutzer die folgenden Funktionen aus:

- Deaktivieren des Benutzerkontos.
- Anhängen des folgenden Suffixes an den Benutzernamen: **- Deprovisioniert**, gefolgt von dem Datum, an dem die Bereitstellung für das Benutzerkonto zurückgenommen wurde.

Beispielsweise ändert die Richtlinie den Benutzernamen **John Smith** in **John Smith – Deprovisioniert am 12/11/2010**.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Bei der Deprovisionierung für ein Benutzerkonto in dem Container, den Sie in Schritt 2 ausgewählt haben, deaktiviert Quest One ActiveRoles folglich das Benutzerkonto und benennt es um, wie von dieser Richtlinie vorgeschrieben.

In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten „Neues Deprovisionsrichtlinienobjekt" erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter Erstellen eines Richtlinienobjekts im Abschnitt Verwaltungsaufgaben für Richtlinienobjekte weiter oben in diesem Kapitel.

Um die Richtlinie zu konfigurieren, klicken Sie auf **Benutzerkonto-Deprovisionierung** auf der Seite **Auswählen des Richtlinientyps** des Assistenten. Klicken Sie dann auf **Weiter**.

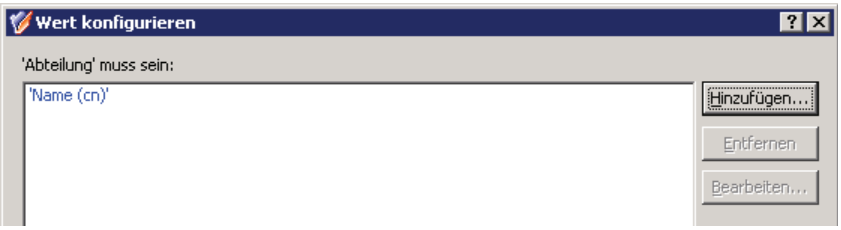
Aktivieren Sie auf der Seite **Optionen zur Verhinderung der Anmeldung** die folgenden Kontrollkästchen:

- **Benutzerkonto deaktivieren**
- **Benutzerkonto umbenennen in**

Klicken Sie dann auf die Schaltfläche **Konfigurieren**, und schließen Sie das Dialogfeld **Wert konfigurieren** anhand der folgenden Anweisungen ab.

1. Klicken Sie auf **Hinzufügen**.
2. Klicken Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** auf **Benutzereigenschaft**, und konfigurieren Sie den Eintrag wie folgt:
   a) Klicken Sie auf **Auswählen** und wählen Sie die Eigenschaft **Name** aus.
   b) Klicken Sie auf **Alle Zeichen des Eigenschaftswerts**.
   c) Klicken Sie auf **OK**.
3. Klicken Sie auf **Hinzufügen**.
4. Klicken Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** auf **Text**, und konfigurieren Sie den Eintrag wie folgt:
   a) Geben Sie im Feld **Textwert** den Wert **– Deprovisioniert** ein.
   b) Klicken Sie auf **OK**.
5. Klicken Sie auf **Hinzufügen**.
6. Klicken Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** auf **Datum und Uhrzeit**, und konfigurieren Sie den Eintrag wie folgt:
   a) Wählen Sie in der Liste unter **Datums- und Zeitformat** das Format **M/T/JJJJ** aus.
   b) Klicken Sie auf **OK**.

Nach dem Ausführen dieser Schritte sollte die Liste der Einträge im Dialogfeld **Wert konfigurieren** der folgenden Abbildung ähneln.



Klicken Sie auf **OK**, um das **Dialogfeld Wert** konfigurieren zu schließen. Klicken Sie dann auf **Weiter** und befolgen Sie die Anweisungen im Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten für neues Deprovisionsrichtlinienobjekt anwenden, oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen bezüglich der Anwendung eines Richtlinienobjekts finden Sie unter Anwenden von Richtlinienobjekten und Verwalten des Richtlinienbereichs weiter oben in diesem Kapitel.

Szenario 2: Verwaltete Einheit zum Ablegen deprovisionierter Benutzerkonten

In diesem Szenario wird beschrieben, wie Sie eine verwaltete Einheit und die Richtlinie „Benutzerkontodeprovisionierung" so konfigurieren, dass die verwaltete Einheit alle deprovisionierten Benutzerkonten enthält. Die Richtlinie legt bei der Deprovisionierung für einen Benutzer die Eigenschaft **Hinweise** auf **Deprovisioniert** fest. Die verwaltete Einheit wiederum ist so konfiguriert, dass sie Benutzerkonten einschließt, deren Eigenschaft **Hinweise** auf **Deprovisioniert** festgelegt ist.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie die verwaltete Einheit.
2. Konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
3. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Nach der Deprovisionierung für ein Benutzerkonto in dem Container, den Sie in Schritt 3 ausgewählt haben, fügt Quest One ActiveRoles folglich dieses Konto automatisch der in Schritt 1 erstellten verwalteten Einheit hinzu.

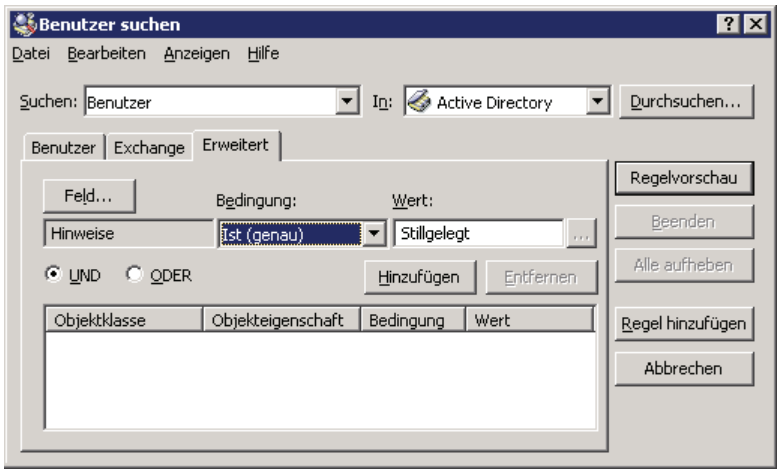
In den folgenden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren der verwalteten Einheit

Sie können die verwaltete Einheit mittels der Quest One ActiveRoles-Konsole erstellen und konfigurieren:

1. Klicken Sie in der Konsolenstruktur unter **Configuration** Klicken Sie mit der rechten Maustaste auf **Verwaltete Einheiten** und wählen Sie **Neu | Verwaltete Einheit**.
2. Geben Sie in das Feld **Name** einen Namen für die verwaltete Einheit ein. Sie können beispielsweise **Deprovisionierte Benutzer** eingeben.
3. Klicken Sie auf **Weiter**.
4. Konfigurieren Sie wie folgt die Mitgliedschaftsregel so, dass die verwaltete Einheit die deprovisionierten Benutzerkonten aus allen bei Quest One ActiveRoles registrierten Domänen (den verwalteten Domänen) enthält:
   a) Klicken Sie auf der Seite des Assistenten auf **Hinzufügen**.
   b) Klicken Sie im Dialogfeld **Mitgliedschaftsregeltyp** auf **Nach Abfrage einschließen** und klicken Sie dann auf **OK**.
   c) Richten Sie im Fenster **Mitgliedschaftsregel erstellen** die Regel ein:
      - Klicken Sie unter **Suchen** auf **Benutzer**.
      - Klicken Sie auf **Durchsuchen** und wählen Sie **Active Directory**.
      - Klicken Sie auf die Registerkarte **Erweitert**.
      - Klicken Sie auf die Schaltfläche **Feld** und dann auf **Hinweise**.
      - Klicken Sie unter **Bedingung** auf **Ist (genau)**.
      - Geben Sie unter **Wert** den Wert **Deprovisioniert** ein.

Nun sollte das Fenster der folgenden Abbildung entsprechen:



- Klicken Sie auf die Schaltfläche **Hinzufügen**.
- Klicken Sie auf die Schaltfläche **Regel hinzufügen**.

d) Klicken Sie auf der Seite des Assistenten auf **Hinzufügen**.

e) Klicken Sie im Dialogfeld **Mitgliedschaftsregeltyp** auf **Deprovisionierte beibehalten** und klicken Sie dann auf **OK**.

5. Klicken Sie auf **Weiter**, wiederum auf **Weiter** und dann auf **Fertig stellen**.

Schritt 2: Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt konfigurieren, indem Sie das Richtlinienobjekt ändern, das das vorige Szenario implementiert; siehe „Szenario 1: Deaktivieren und Umbenennen von Benutzerkonten bei einer Benutzerdeprovisionierung" weiter oben in diesem Abschnitt.

Zeigen Sie das Dialogfeld **Eigenschaften** für dieses Richtlinienobjekt an und öffnen Sie die Registerkarte **Richtlinien**. Wählen Sie dann in der Liste die Richtlinie aus und klicken Sie auf **Anzeigen/Bearbeiten**, um das Dialogfeld **Eigenschaften der Benutzerkonto-Deprovisionierungsrichtlinie** anzuzeigen.

Die Registerkarte **Zu aktualisierende Eigenschaften** im Dialogfeld **Eigenschaften der Benutzerkonto-Deprovisionierungsrichtlinie** ähnelt der Seite **Zu aktualisierende Eigenschaften** des Assistenten, mit dem Sie das Richtlinienobjekt konfiguriert haben. Mit dieser Registerkarte können Sie wie folgt die Aktualisierungsregel für die Eigenschaft **Hinweise** hinzufügen:

1. Klicken Sie auf **Hinzufügen**, um das Dialogfeld **Objekteigenschaft wählen** anzuzeigen.
2. Aktivieren Sie das Kontrollkästchen neben der Eigenschaft **Hinweise** und klicken Sie dann auf **OK**.
3. Geben Sie im Dialogfeld **Wert hinzufügen Deprovisioned** in das Feld **'Hinweise' muss sein** ein und klicken Sie dann auf **OK**.

Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften der Benutzerkonto-Deprovisionierungsrichtlinie** zu schließen.

Schritt 3: Anwenden des Richtlinienobjekts

Um das Richtlinienobjekt anzuwenden, können Sie im Dialogfeld **Eigenschaften** für dieses Richtlinienobjekt die Registerkarte **Bereich** verwenden:

1. Klicken Sie auf der Registerkarte **Bereich** auf die Schaltfläche **Bereich**, um das Fenster **Quest One ActiveRoles-Richtlinienbereich** für das zu verwaltende Richtlinienobjekt anzuzeigen.
2. Klicken Sie auf **Hinzufügen** und wählen Sie die Domäne, Organisationseinheit oder verwaltete Einheit aus, auf die Sie die Richtlinie anwenden möchten.

   *Sie können auch mit Hilfe der Schaltfläche **Entfernen** Elemente entfernen, auf die die Richtlinie nicht mehr angewendet werden soll.*
3. Klicken Sie auf **OK**, um das Fenster **Quest One ActiveRoles-Richtlinienbereich** zu schließen.
4. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** für das Richtlinienobjekt zu schließen.

Weitere Informationen bezüglich der Anwendung eines Richtlinienobjekts finden Sie unter Anwenden von Richtlinienobjekten und Verwalten des Richtlinienbereichs weiter oben in diesem Kapitel.

Entfernung der Gruppenmitgliedschaft

Richtlinien dieser Kategorie dienen zur Automatisierung des Entfernens von deprovisionierten Benutzerkonten. Eine Richtlinie kann so konfiguriert werden, dass sie Benutzerkonten aus allen Gruppen entfernt, dabei jedoch optional Ausnahmen macht. Einzelne Richtlinienregeln können auf Sicherheits gruppen und auf E-Mail-fähige Gruppen vom Sicherheits- oder Verteilungstyp angewandt werden.

Funktionsweise dieser Richtlinie

Beim Verarbeiten einer Deprovisionsanforderung für einen Benutzer verwendet Quest One ActiveRoles diese Richtlinie, um zu bestimmen, welche Änderungen an Gruppenmitgliedschaften des Benutzerkontos vorgenommen werden sollen. Indem sie das Konto aus Sicherheitsgruppen entfernt, widerruft die Richtlinie Zugriffsrechte des Benutzers für Ressourcen. Indem sie das Konto aus E-Mail-fähigen Gruppen entfernt, verhindert die Richtlinie fehlerhafte Situationen, in denen E-Mail an das deprovisionierte Postfach gesendet wird.

Die Benutzer, für die die Bereitstellung zurückgenommen wurde, werden automatisch aus allen dynamischen Gruppen entfernt, unabhängig von den Einstellungen der Richtlinie „Entfernen der Gruppenmitgliedschaft".

Die Richtlinie zur Entfernung der Gruppenmitgliedschaft enthält separate Regeln für Sicherheitsgruppen und E-Mail-fähige Gruppen. Für jede Kategorie von Gruppen kann Quest One ActiveRoles anhand einer Regel eine der Aktionen ausführen, die in der folgenden Tabelle zusammengefasst sind.

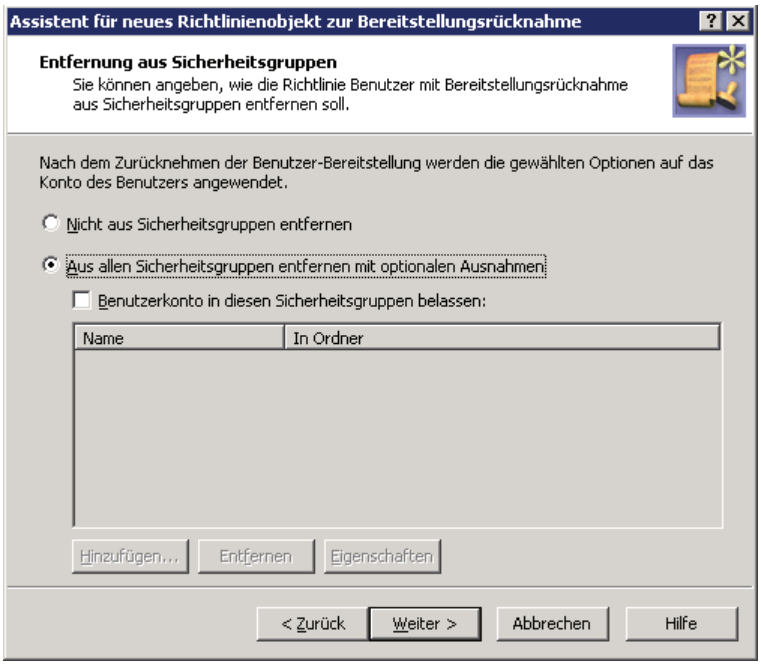
KATEGORIE	AKTION	ERGEBNIS
Sicherheits-gruppen	Kein Entfernen aus Gruppen	Der Benutzer, für den die Bereitstellung zurückgenommen wurde, verbleibt in allen Sicherheitsgruppen, in denen zum Zeitpunkt der Zurücknahme eine Mitgliedschaft bestand, außer in den dynamischen Gruppen.
	Entfernen aus allen Gruppen	Der Benutzer, für den die Bereitstellung zurückgenommen wurde, wird aus allen Sicherheitsgruppen entfernt.
	Entfernen aus allen Gruppen außer den angegebenen	Der Benutzer, für den die Bereitstellung zurückgenommen wurde, wird aus den angegebenen Sicherheitsgruppen nicht entfernt, außer aus dynamischen Gruppen. Aus allen anderen Sicherheitsgruppen wird der Benutzer entfernt.
Mail-aktivierte Gruppen	Kein Entfernen aus Gruppen	Der Benutzer, für den die Bereitstellung zurückgenommen wurde, verbleibt in den Verteilergruppen und E-Mail-fähigen Gruppen, außer in den dynamischen Gruppen.
	Entfernen aus allen Gruppen	Der Benutzer, für den die Bereitstellung zurückgenommen wurde, wird aus allen Verteilergruppen und allen E-Mail-fähigen Sicherheitsgruppen entfernt.
	Entfernen aus allen Gruppen außer den angegebenen	Der Benutzer, für den die Bereitstellung zurückgenommen wurde, wird aus den angegebenen Verteilergruppen und E-Mail-fähigen Sicherheitsgruppen nicht entfernt, außer aus dynamischen Gruppen. Aus allen anderen Verteilergruppen und E-Mail-fähigen Sicherheitsgruppen wird der Benutzer entfernt.

Bei einem Konflikt in der Richtlinienimplementierung hat die Entfernungsaktion Vorrang. Beispielsweise wird mit einer Regel, die für das Entfernen des Benutzerkontos aus allen Sicherheitsgruppen konfiguriert ist, das Benutzerkonto auch dann aus allen Sicherheitsgruppen entfernt, wenn eine weitere Regel vorhanden ist, die angibt, dass Quest One ActiveRoles das Benutzerkonto aus E-Mail-fähigen Sicherheitsgruppen nicht entfernen soll.

Ein weiterer Konflikt kann auftreten, wenn eine Richtlinie dieser Kategorie versucht, einen deprovisionierten Benutzer aus einer Gruppe zu entfernen, die als dynamische Gruppe von Quest One ActiveRoles konfiguriert ist (siehe das Kapitel „Dynamische Gruppen" weiter unten in diesem Dokument). Die Richtlinie für dynamische Gruppen erkennt, dass der Benutzer entfernt wurde, und kann den Benutzer wieder zur dynamischen Gruppe hinzufügen. Um eine solche Situation zu vermeiden, lässt Quest One ActiveRoles nicht zu, dass dynamische Gruppen deprovisionierte Benutzer enthalten. Nach der Deprovisionierung wird das Konto des Benutzers aus allen dynamischen Gruppen entfernt.

Konfigurieren der Richtlinie „Entfernen der Gruppenmitgliedschaft"

Um die Richtlinie „Entfernen der Gruppenmitgliedschaft" zu konfigurieren, wählen Sie **Entfernen der Gruppenmitgliedschaft** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten „Neues Deprovisionsrichtlinienobjekt" oder im Assistenten „Deprovisionsrichtlinie hinzufügen" aus. Klicken Sie dann auf **Weiter**, damit die Seite **Entfernung aus Sicherheitsgruppen** angezeigt wird.


Assistent für neues Richtlinienobjekt zur Bereitstellungsrücknahme
Entfernung aus Sicherheitsgruppen
Sie können angeben, wie die Richtlinie Benutzer mit Bereitstellungsrücknahme aus Sicherheitsgruppen entfernen soll.
Nach dem Zurücknehmen der Benutzer-Bereitstellung werden die gewählten Optionen auf das Konto des Benutzers angewendet.
Nicht aus Sicherheitsgruppen entfernen
Aus allen Sicherheitsgruppen entfernen mit optionalen Ausnahmen:
Benutzerkonto in diesen Sicherheitsgruppen belassen:
Name
In Ordner
Hinzufügen...
Entfernen
Eigenschaften
< Zurück
Weiter >
Abbrechen
Hilfe

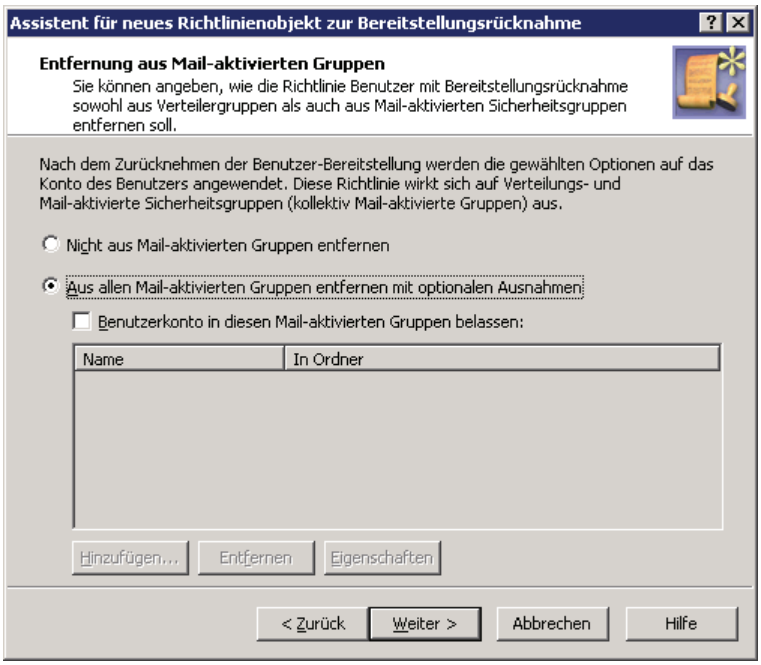
Auf dieser Seite können Sie eine Regel konfigurieren, die angibt, wie ein Benutzer mit zurückgenommener Bereitstellung aus Sicherheitsgruppen entfernt werden soll.

Wählen Sie eine der folgenden Optionen aus:

- Klicken Sie auf **Nicht aus Sicherheitsgruppen entfernen**, damit die Richtlinie keine Änderungen an Sicherheitsgruppen-Mitgliedschaften beim Benutzerkonto vornimmt.
- Klicken Sie auf **Aus allen Sicherheitsgruppen entfernen mit optionalen Ausnahmen**, damit die Richtlinie das Benutzerkonto aus allen Sicherheitsgruppen entfernt.

Mit der zweiten Option können Sie angeben, ob die Richtlinie das Objekt in bestimmten Sicherheitsgruppen belassen soll. Um eine Liste solcher Gruppen einzurichten, aktivieren Sie das Kontrollkästchen **Benutzerkonto in diesen Sicherheitsgruppen belassen**, klicken Sie dann auf die Schaltfläche **Hinzufügen** und wählen Sie die Gruppen aus, die Sie in die Liste einschließen möchten.

Klicken Sie nach dem Konfigurieren der Regel für Sicherheitsgruppen auf **Weiter**, um die Seite **Entfernung aus Mail-aktivierten Gruppen** anzuzeigen.


Assistent für neues Richtlinienobjekt zur Bereitstellungsrücknahme
Entfernung aus Mail-aktivierten Gruppen
Sie können angeben, wie die Richtlinie Benutzer mit Bereitstellungsrücknahme sowohl aus Verteilergruppen als auch aus Mail-aktivierten Sicherheitsgruppen entfernen soll.
Nach dem Zurücknehmen der Benutzer-Bereitstellung werden die gewählten Optionen auf das Konto des Benutzers angewendet. Diese Richtlinie wirkt sich auf Verteilungs- und Mail-aktivierte Sicherheitsgruppen (kollektiv Mail-aktivierte Gruppen) aus.
Nicht aus Mail-aktivierten Gruppen entfernen
Aus allen Mail-aktivierten Gruppen entfernen mit optionalen Ausnahmen
Benutzerkonto in diesen Mail-aktivierten Gruppen belassen:
Name
In Ordner
Hinzufügen...
Entfernen
Eigenschaften
< Zurück
Weiter >
Abbrechen
Hilfe

Diese Seite ähnelt der vorigen. Sie ermöglicht das Konfigurieren einer Regel, anhand derer ein Benutzerkonto sowohl aus Verteilergruppen als auch aus E-Mail-fähigen Sicherheitsgruppen entfernt wird. Diese Gruppen werden zusammen als E-Mail-fähige Gruppen bezeichnet.

Wählen Sie eine der folgenden Optionen aus:

- Klicken Sie auf **Nicht aus Mail-aktivierten Gruppen entfernen**, damit die Richtlinie keine Änderungen an E-Mail-fähigen Gruppenmitgliedschaften beim Benutzerkonto vornimmt.
- Klicken Sie auf **Aus allen Mail-aktivierten Gruppen entfernen mit optionalen Ausnahmen**, damit die Richtlinie das Benutzerkonto aus allen E-Mail-fähigen Gruppen entfernt.

Mit der zweiten Option können Sie angeben, ob die Richtlinie das Objekt in bestimmten E-Mail-fähigen Gruppen belassen soll. Um eine Liste solcher Gruppen einzurichten, aktivieren Sie das Kontrollkästchen **Benutzerkonto in diesen Mail-aktivierten Gruppen belassen**, klicken Sie dann auf die Schaltfläche **Hinzufügen** und wählen Sie die Gruppen aus, die Sie in die Liste einschließen möchten.

Klicken Sie nach dem Konfigurieren der Regel für E-Mail-fähige Gruppen auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Verfahren zum Konfigurieren einer Richtlinie zum Entfernen einer Gruppenmitgliedschaft

So konfigurieren Sie eine Richtlinie zur Entfernung der Gruppenmitgliedschaft:

1. Wählen Sie auf der Seite **Zu konfigurierende Richtlinie** die Option **Entfernen der Gruppenmitgliedschaft** und klicken Sie dann auf **Weiter**.
2. Führen Sie auf der Seite **Entfernung aus Sicherheitsgruppen** einen der folgenden Vorgänge aus:
   - Klicken Sie auf **Nicht aus Sicherheitsgruppen entfernen**, damit die Richtlinie keine Änderungen an Sicherheitsgruppen-Mitgliedschaften beim Benutzerkonto vornimmt.
   - Klicken Sie auf **Aus allen Sicherheitsgruppen entfernen mit optionalen Ausnahmen**, damit die Richtlinie das Benutzerkonto aus allen Sicherheitsgruppen entfernt.
3. Wenn Sie die zweite Option in Schritt 2 ausgewählt haben, geben Sie an, ob die Richtlinie das Objekt in bestimmten Sicherheitsgruppen belassen soll. Führen Sie einen der nachfolgend aufgeführten Schritte aus:
   - Aktivieren Sie das Kontrollkästchen **Benutzerkonto in diesen Sicherheitsgruppen belassen** und erstellen Sie die Liste der Sicherheitsgruppen, in denen die Richtlinie das Benutzerkonto belassen soll.
   - Wenn die Richtlinie das Benutzerkonto aus allen Sicherheitsgruppen entfernen soll, lassen Sie das Kontrollkästchen deaktiviert.
4. Klicken Sie auf **Weiter**.
5. Führen Sie auf der Seite **Entfernung aus E-Mail-fähigen Gruppen** einen der folgenden Vorgänge aus:
   - Klicken Sie auf **Nicht aus Mail-aktivierten Gruppen entfernen**, damit die Richtlinie keine Änderungen an E-Mail-fähigen Gruppenmitgliedschaften beim Benutzerkonto vornimmt.
   - Klicken Sie auf **Aus allen Mail-aktivierten Gruppen entfernen mit optionalen Ausnahmen**, damit die Richtlinie das Benutzerkonto aus allen E-Mail-fähigen Gruppen entfernt.
6. Wenn Sie die zweite Option in Schritt 5 ausgewählt haben, geben Sie an, ob die Richtlinie das Objekt in bestimmten E-Mail-fähigen Gruppen belassen soll. Führen Sie einen der nachfolgend aufgeführten Schritte aus:
   - Aktivieren Sie das Kontrollkästchen **Benutzerkonto in diesen E-Mail-aktivierten Gruppen belassen** und erstellen Sie die Liste der E-Mail-fähigen Gruppen, in denen die Richtlinie das Benutzerkonto belassen soll.
   - Wenn die Richtlinie das Benutzerkonto aus allen E-Mail-fähigen Gruppen entfernen soll, lassen Sie das Kontrollkästchen deaktiviert.
7. Klicken Sie auf **Weiter**.
8. Auf der Seite **Richtlinie erzwingen** können Sie Objekte angeben, auf die dieses Richtlinienobjekt angewandt werden soll:
   - Klicken Sie auf **Hinzufügen** und verwenden Sie das Objekt **Objekte auswählen**, um die gewünschten Objekte auszuwählen.
9. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Szenario: Entfernen von Benutzern mit zurückgenommener Bereitstellung aus allen Gruppen

Die in diesem Szenario beschriebenen Richtlinie entfernt die Benutzer mit zurückgenommener Bereitstellung aus allen Gruppen, also aus Sicherheits- und Verteilergruppen.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Bei der Deprovisionierung für ein Benutzerkonto in dem Container, den Sie in Schritt 2 ausgewählt haben, entfernt Quest One ActiveRoles folglich das Benutzerkonto aus allen Gruppen.

In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten „Neues Deprovisionsrichtlinienobjekt" erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter Erstellen eines Richtlinienobjekts im Abschnitt Verwaltungsaufgaben für Richtlinienobjekte weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Richtlinientyp auswählen** des Assistenten auf **Entfernen der Gruppenmitgliedschaft**. Klicken Sie dann auf **Weiter**, und führen Sie die folgenden Schritte aus:

1. Auf der Seite **Entfernung aus Sicherheitsgruppen**:
   a) Klicken Sie auf **Aus allen Sicherheitsgruppen entfernen mit optionalen Ausnahmen**.
   b) Stellen Sie sicher, dass das Kontrollkästchen **Benutzerkonto in diesen Sicherheitsgruppen belassen** deaktiviert ist.
   c) Klicken Sie auf **Weiter**.
2. Auf der Seite **Entfernung aus Mail-aktivierten Gruppen**:
   a) Klicken Sie auf **Aus allen Mail-aktivierten Gruppen entfernen mit optionalen Ausnahmen**.
   b) Stellen Sie sicher, dass das Kontrollkästchen **Benutzerkonto in diesen E-Mail aktivierten Gruppen belassen** deaktiviert ist.
   c) Klicken Sie auf **Weiter**.
3. Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten für neues Deprovisionsrichtlinienobjekt anwenden, oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen bezüglich der Anwendung eines Richtlinienobjekts finden Sie unter Anwenden von Richtlinienobjekten und Verwalten des Richtlinienbereichs weiter oben in diesem Kapitel.

Exchange-Postfach-Deprovisionierung

Richtlinien dieser Kategorie dienen zum Automatisieren der folgenden Aufgaben, mit denen für deprovisionierte Benutzer Microsoft Exchange-Ressourcen deprovisioniert werden:

- Verbergen von deprovisionierten Benutzern in Adressenlisten
- Verhindern, dass Unzustellbarkeitsberichte gesendet werden
- Gewähren des Vollzugriffs für ausgewählte Personen auf deprovisionierte Postfächer
- Umleiten von E-Mails, die an deprovisionierte Benutzer gerichtet sind

Beim Konfigurieren einer Richtlinie dieser Kategorie geben Sie an, wie Quest One ActiveRoles das Konto und das Postfach des Benutzers ändern soll, wenn für den Benutzer eine Deprovisionsanforderung vorliegt. Damit wird bezweckt, dass weniger E-Mails an diesen Benutzer gesendet werden und dass ausgewählte Personen zum Überwachen solcher E-Mails autorisiert werden.

Funktionsweise dieser Richtlinie

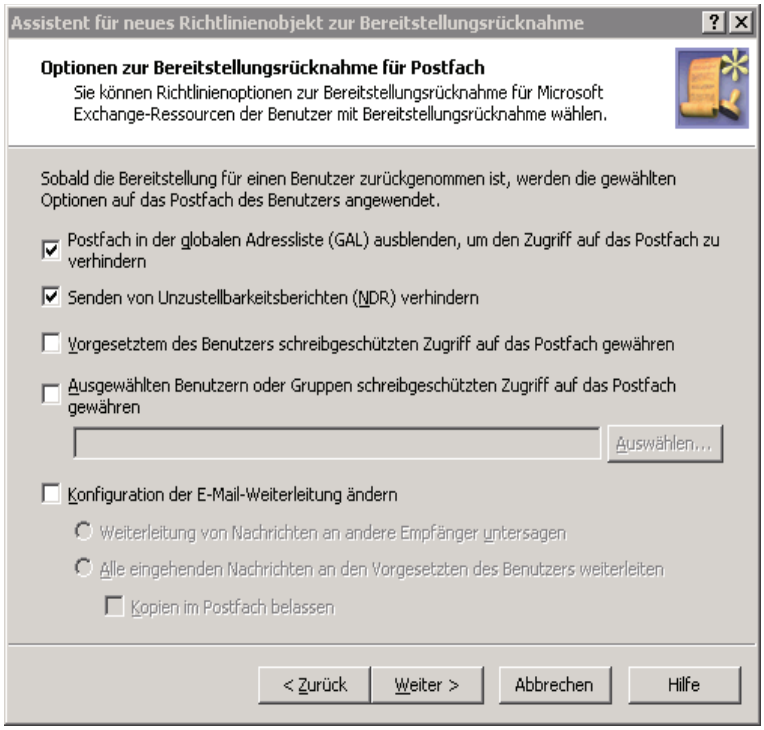
Beim Verarbeiten einer Deprovisionsanforderung für einen Benutzer verwendet Quest One ActiveRoles diese Richtlinie, um die Optionen für die Deprovisionierung von Exchange-Postfach zu bestimmen, und aktualisiert das Konto sowie das Postfach des Benutzers dann entsprechend.

Die verfügbaren Optionen für die Postfachdeprovisionierung werden in der folgenden Tabelle zusammengefasst. Für jede Option wird in der Tabelle die Auswirkung der Richtlinie auf das Benutzerpostfach umrissen.

OPTION	AUSWIRKUNG DER RICHTLINIE
Ausblenden des Postfachs aus der globalen Adressliste	Verhindert, dass der deprovisionierte Benutzer in der Exchange-Adressenliste der Organisation angezeigt wird. Wenn Sie diese Option aktivieren, wird der Benutzer in allen Adressenlisten verborgen. Diese Option hebt die Verfügbarkeit des Postfachs auf. Sie können sich nicht als der Postfachbenutzer bei Exchange Server anmelden und nicht anderweitig auf das verborgene Postfach zugreifen.
Senden von Unzustellbarkeitsberichten (NDR) verhindern	Verhindert, dass Unzustellbarkeitsberichte generiert werden, wenn E-Mails an das deprovisionierte Postfach gesendet werden. (Bei einem Unzustellbarkeitsbericht handelt es sich um die Benachrichtigung, dass eine Nachricht nicht an den Empfänger übermittelt wurde).
Vorgesetztem des Benutzers schreibgeschützten Zugriff auf das Postfach gewähren	Gewährt der Person, die als Vorgesetzter des deprovisionierten Benutzers angegeben ist, Vollzugriff auf das Postfach dieses Benutzers. Der Vorgesetzte wird anhand des Attributs **Vorgesetzter** des deprovisionierten Benutzerkontos in Active Directory bestimmt.
Ausgewählten Benutzern oder Gruppen schreibgeschützten Zugriff auf das Postfach gewähren	Gewährt den angegebenen Benutzern oder Gruppen Vollzugriff auf das Postfach des deprovisionierten Benutzers.
Weiterleiten von Nachrichten verbieten	Für diesen Benutzer bestimmte E-Mails werden nicht an einen alternativen Empfänger weitergeleitet.
Weiterleiten aller eingehenden Nachrichten an den Vorgesetzten des Benutzers	Für diesen Benutzer bestimmte E-Mails werden an den Vorgesetzten des Benutzers weitergeleitet. Der Vorgesetzte wird anhand des Attributs **Vorgesetzter** des deprovisionierten Benutzerkontos in Active Directory bestimmt.
Kopien im Postfach belassen	Für diesen Benutzer bestimmte E-Mails werden an des Postfach das Benutzers und des Vorgesetzten übermittelt. Wenn Sie diese Option nicht aktivieren, werden solche E-Mails nur an das Postfach des Vorgesetzten übermittelt.

Konfigurieren der Richtlinie „Deprovisionierung des Exchange-Postfachs“

Um die Richtlinie „Deprovisionierung des Exchange-Postfachs“ zu konfigurieren, wählen Sie **Deprovisionierung des Exchange-Postfachs** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten „Neues Deprovisionsrichtlinienobjekt“ oder im Assistenten „Deprovisionsrichtlinie hinzufügen“ aus. Klicken Sie dann auf **Weiter**, um die Seite **Optionen zur Bereitstellungsrücknahme für Postfach** anzuzeigen:


Assistent für neues Richtlinienobjekt zur Bereitstellungsrücknahme
Optionen zur Bereitstellungsrücknahme für Postfach
Sie können Richtlinienoptionen zur Bereitstellungsrücknahme für Microsoft Exchange-Ressourcen der Benutzer mit Bereitstellungsrücknahme wählen.
Sobald die Bereitstellung für einen Benutzer zurückgenommen ist, werden die gewählten Optionen auf das Postfach des Benutzers angewendet.
Postfach in der globalen Adressliste (GAL) ausblenden, um den Zugriff auf das Postfach zu verhindern
Senden von Unzustellbarkeitsberichten (NDR) verhindern
Vorgesetztem des Benutzers schreibgeschützten Zugriff auf das Postfach gewähren
Ausgewählten Benutzern oder Gruppen schreibgeschützten Zugriff auf das Postfach gewähren
Auswählen...
Konfiguration der E-Mail-Weiterleitung ändern
Weiterleitung von Nachrichten an andere Empfänger untersagen
Alle eingehenden Nachrichten an den Vorgesetzten des Benutzers weiterleiten
Kopien im Postfach belassen
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite können Sie die Optionen für die Deprovisionierung von Exchange-Postfach für den Stammordner auswählen, die Quest One ActiveRoles bei der Deprovisionierung für einen Benutzer anwenden soll. Die Namen der ersten vier Optionen sind selbsterklärend (siehe auch Tabelle oben):

- Postfach in der globalen Adressliste (GAL) ausblenden, um den Zugriff auf das Postfach zu verhindern
- Senden von Unzustellbarkeitsberichten (NDR) verhindern
- Vorgesetztem des Benutzers schreibgeschützten Zugriff auf das Postfach gewähren
- Ausgewählten Benutzern oder Gruppen schreibgeschützten Zugriff auf das Postfach gewähren

Aktivieren Sie die Kontrollkästchen neben den Optionen, die angewendet werden sollen. Für die vierte Option müssen Sie auf die Schaltfläche **Auswählen** klicken, um Benutzer oder Gruppen auszuwählen. Die ausgewählten Benutzer und Gruppen werden autorisiert, auf die Postfächer der Benutzer mit zurückgenommener Bereitstellung zuzugreifen.

Sie können die Richtlinie auch so konfigurieren, dass sie die Weiterleitungsadresse für die deprovisionierten Benutzer ändert. Wenn Sie das Kontrollkästchen **Konfiguration der E-Mail Weiterleitung ändern** aktivieren, setzt die Richtlinie die Weiterleitungsadresse auf eine der folgenden Adressen:

- **Keine.** Um anzugeben, dass die an einen deprovisionierten Benutzer adressierten E-Mail-Nachrichten nicht weitergeleitet werden sollen, klicken Sie auf **Weiterleitung von Nachrichten an andere Empfänger untersagen**.
- **Verwalter des Benutzers.** Um anzugeben, dass die an einen deprovisionierten Benutzer adressierten E-Mail-Nachrichten an den Vorgesetzten dieses Benutzers gesendet sollen, klicken Sie auf **Alle eingehenden Nachrichten an den Vorgesetzten des Benutzers weiterleiten**.

Mit der zweiten Option können Sie angeben, ob E-Mail-Nachrichten an den Benutzer mit zurückgenommener Bereitstellung an das Postfach des Benutzers übermittelt werden sollen:

- Wenn Sie das Kontrollkästchen **Kopien im Postfach belassen** aktivieren, werden die Nachrichten an des Postfach des Benutzers und des Vorgesetzten übermittelt.
- Wenn Sie das Kontrollkästchen **Kopien im Postfach belassen** deaktivieren, werden die Nachrichten nur an das Postfach des Vorgesetzten übermittelt.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Verfahren zum Konfigurieren einer Deprovisionierungsrichtlinie für Exchange-Postfächern

So konfigurieren Sie eine Richtlinie zur Deprovisionierung von Exchange-Postfächern:

1. Wählen Sie auf der Seite **Zu konfigurierende Richtlinie** die Option **Deprovisionierung des Exchange-Postfachs** und klicken Sie dann auf **Weiter**.
2. Wählen Sie auf der Seite **Optionen zur Bereitstellungsrücknahme für Postfach** die Optionen aus, die die Richtlinie anwenden soll, wenn Sie ein Benutzerkonto deprovisioniert. Sie können jede beliebige Kombination dieser Optionen auswählen, um Microsoft Exchange-Ressourcen für das deprovisionierte Benutzerkonto zu deprovisionieren.
   - Ausblenden des Postfachs aus der globalen Adressliste
   - Senden von Unzustellbarkeitsberichten (NDR) verhindern
   - Vorgesetztem des Benutzers schreibgeschützten Zugriff auf das Postfach gewähren
   - Ausgewählten Benutzern oder Gruppen schreibgeschützten Zugriff auf das Postfach gewähren
   - Konfiguration der E-Mail-Weiterleitung ändern
3. Wenn Sie das Kontrollkästchen **Den ausgewählten Benutzern oder Gruppen Vollzugriff auf das Postfach gewähren** aktiviert haben, klicken Sie auf **Wählen** und verwenden Sie das Dialogfeld **Objekte auswählen**, um die gewünschten Benutzer oder Gruppen anzugeben.
4. Wenn Sie das Kontrollkästchen **Konfiguration der E-Mail-Weiterleitung ändern** aktiviert haben, führen Sie eine der folgenden Aktionen durch:
   - Klicken Sie auf **Weiterleitung von Nachrichten an andere Empfänger untersagen**, um anzugeben, dass die an den deprovisionierten Benutzer gesendeten E-Mail-Nachrichten nicht weitergeleitet werden sollen.
   - Klicken Sie auf **Alle eingehenden Nachrichten an den Vorgesetzten des Benutzers weiterleiten**, um anzugeben, dass die an den deprovisionierten Benutzer gesendeten E-Mail-Nachrichten an den Vorgesetzten dieses Benutzers gesendet werden sollen.

Aktivieren bzw. deaktivieren Sie dann das Kontrollkästchen **Kopien im Postfach belassen**, um anzugeben, ob die Nachrichten sowohl an das Postfach des Benutzers als auch an das Postfach des Vorgesetzten oder nur an das Postfach des Vorgesetzten gesendet werden sollen.

5. Klicken Sie auf **Weiter**.
6. Auf der Seite **Richtlinie erzwingen** können Sie Objekte angeben, auf die dieses Richtlinienobjekt angewandt werden soll:
   - Klicken Sie auf **Hinzufügen** und verwenden Sie das Objekt **Objekte auswählen**, um die gewünschten Objekte auszuwählen.
7. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Szenario: Ausblenden eines Postfachs und Weiterleiten der E-Mails an den Vorgesetzten

Die in diesem Szenario beschriebene Richtlinie führt während der Deprovisionierung für einen Benutzer die folgenden Funktionen aus:

- Blendet den Benutzer mit zurückgenommener Bereitstellung in den Exchange-Adressenlisten der Organisation aus.
- Konfiguriert die E-Mail-Weiterleitung so, dass E-Mail-Nachrichten an den Benutzer mit zurückgenommener Bereitstellung an den Vorgesetzten des Benutzers gesendet werden, nicht jedoch an das Postfach des Benutzers.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Bei der Deprovisionierung für ein Benutzerkonto in dem Container, den Sie in Schritt 2 ausgewählt haben, blendet Quest One ActiveRoles folglich den Benutzer in den Exchange-Adressenlisten aus und konfiguriert die Weiterleitungsadresse für den Benutzer gemäß der Vorschrift in dieser Richtlinie.

In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten „Neues Deprovisionsrichtlinienobjekt" erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter Erstellen eines Richtlinienobjekts im Abschnitt Verwaltungsaufgaben für Richtlinienobjekte weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Richtlinientyp auswählen** des Assistenten auf **Deprovisionierung des Exchange-Postfachs**. Klicken Sie dann auf **Weiter**.

Aktivieren Sie auf der Seite **Optionen für die Deprovisionierung des Postfachs** die folgenden Kontrollkästchen:

- **Postfach in der globalen Adressliste (GAL) ausblenden, um den Zugriff auf das Postfach zu verhindern**
- **Konfiguration der E-Mail-Weiterleitung ändern**

Stellen sie sicher, dass keine anderen Kontrollkästchen auf der Seite aktiviert sind. Klicken Sie dann auf **Alle eingehenden Nachrichten an den Vorgesetzten des Benutzers weiterleiten**, und deaktivieren Sie das Kontrollkästchen **Kopien im Postfach belassen**.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten für neues Deprovisionsrichtlinienobjekt anwenden, oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen bezüglich der Anwendung eines Richtlinienobjekts finden Sie unter Anwenden von Richtlinienobjekten und Verwalten des Richtlinienbereichs weiter oben in diesem Kapitel.

Stammordner-Deprovisionierung

Richtlinien dieser Kategorie dienen zum Automatisieren der folgenden Aufgaben, mit denen für deprovisionierte Benutzer Stammordner deprovisioniert werden:

- Entziehen des Zugriffs auf Stammordner für deprovisionierte Benutzerkonten
- Gewähren des Lesezugriffs für ausgewählte Personen auf deprovisionierte Stammordner
- Ändern des Besitzers für deprovisionierte Stammordner
- Löschen deprovisionierter Stammordner

Beim Konfigurieren einer Richtlinie dieser Kategorie geben Sie an, wie Quest One ActiveRoles bei einer Deprovisionsanforderung für einen Benutzer die Sicherheit für den Stammordner des Benutzers ändern soll und ob Quest One ActiveRoles beim Löschen eines Benutzerkontos auch Stammordner löschen soll. Damit wird bezweckt, dass deprovisionierte Benutzer am Zugreifen auf ihre Stammordner gehindert werden und dass ausgewählte Personen zum Zugreifen auf solche Stammordner autorisiert werden.

Funktionsweise dieser Richtlinie

Beim Verarbeiten einer Deprovisionsanforderung für einen Benutzer verwendet Quest One ActiveRoles diese Richtlinie, um die Optionen für die Deprovisionierung des Stammordners zu bestimmen, und aktualisiert die Stammordnerkonfiguration des Benutzers dann entsprechend.

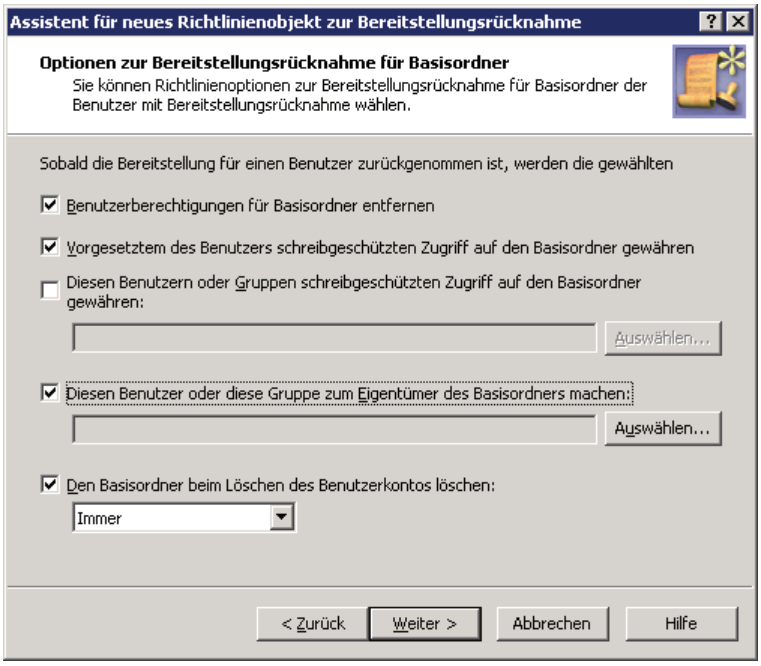
Die verfügbaren Optionen für die Stammordner-Deprovisionierung werden in der folgenden Tabelle zusammengefasst. Für jede Option wird in der Tabelle die Auswirkung der Richtlinie auf den Benutzerstammordner umrissen.

OPTION	AUSWIRKUNG DER RICHTLINIE
Benutzerberechtigungen für Basisordner entfernen	Ändert die Sicherheit für den Stammordner so, dass der Benutzer nicht mehr darauf zugreifen kann.
Vorgesetztem des Benutzers schreibgeschützten Zugriff auf den Stammordner gewähren	Ermöglicht es der Person, die als Vorgesetzter des Benutzers mit zurückgenommener Bereitstellung bezeichnet ist, Daten im Stammordner dieses Benutzers anzuzeigen und abzurufen. Der Vorgesetzte wird anhand des Attributs **Vorgesetzter** des deprovisionierten Benutzerkontos in Active Directory bestimmt.

Ausgewählten Benutzern oder Gruppen schreibgeschützten Zugriff auf den Stammordner gewähren	Ermöglicht es den angegebenen Benutzern oder Gruppen, Daten im Stammordner dieses Benutzers anzuzeigen und abzurufen.
Den ausgewählten Benutzer oder die ausgewählte Gruppe zum Besitzer des Stammordners machen	Legt den ausgewählten Benutzer oder die ausgewählte Gruppe als Besitzer des Stammordners dieses Benutzers fest. Der Besitzer ist dazu autorisiert, die Festlegung von Berechtigungen für den Ordner zu steuern, und kann anderen Berechtigungen erteilen.
Den Basisordner beim Löschen des Benutzerkontos löschen	Analysiert beim Löschen eines Benutzerkontos, ob der Stammordner des Benutzers leer ist, und löscht den Stammordner dann abhängig von der Richtlinienkonfiguration oder behält ihn bei. Eine Richtlinie kann so konfiguriert werden, dass sie nur leere Ordner löscht. Es besteht auch die Option, leere und nicht leere Ordner zu löschen.

Konfigurieren der Richtlinie „Stammordner-Deprovisionierung"

Um eine Stammordner-Deprovisionierungsrichtlinie zu konfigurieren, wählen Sie **Stammordner-Deprovisionierung** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten „Neues Deprovisionsrichtlinienobjekt" oder im Assistenten „Deprovisionsrichtlinie hinzufügen" aus. Klicken Sie dann auf **Weiter**, damit die Seite **Optionen zur Bereitstellungsrücknahme für Basisordner** angezeigt wird.


Assistent für neues Richtlinienobjekt zur Bereitstellungsrücknahme
Optionen zur Bereitstellungsrücknahme für Basisordner
Sie können Richtlinienoptionen zur Bereitstellungsrücknahme für Basisordner der Benutzer mit Bereitstellungsrücknahme wählen.
Sobald die Bereitstellung für einen Benutzer zurückgenommen ist, werden die gewählten
Benutzerberechtigungen für Basisordner entfernen
Vorgesetztem des Benutzers schreibgeschützten Zugriff auf den Basisordner gewähren
Diesen Benutzern oder Gruppen schreibgeschützten Zugriff auf den Basisordner gewähren:
Auswählen...
Diesen Benutzer oder diese Gruppe zum Eigentümer des Basisordners machen:
Auswählen...
Den Basisordner beim Löschen des Benutzerkontos löschen:
Immer
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite können Sie die Deprovisionierungsoptionen für den Stammordner auswählen, die Quest One ActiveRoles bei der Deprovisionierung für einen Benutzer anwenden soll.

Die Namen der ersten vier Optionen sind selbsterklärend. Sie beziehen sich auf die Richtlinienoptionen, die in der Tabelle oben zusammengefasst sind:

- Benutzerberechtigungen für Basisordner entfernen
- Vorgesetztem des Benutzers schreibgeschützten Zugriff auf den Basisordner gewähren
- Diesen Benutzern oder Gruppen schreibgeschützten Zugriff auf den Basisordner gewähren
- Diesen Benutzer oder diese Gruppe zum Eigentümer des Basisordners machen

Aktivieren Sie die Kontrollkästchen neben den Optionen, die angewendet werden sollen.

Für die dritte Option müssen Sie auf die Schaltfläche **Auswählen** klicken, um Benutzer oder Gruppen auszuwählen. Die ausgewählten Benutzer oder Gruppen werden autorisiert, Daten in den Stammordnern der deprovisionierten Benutzer anzuzeigen und abzurufen.

Für die vierte Option müssen Sie auf die Schaltfläche **Auswählen** klicken, um einen Benutzer oder eine Gruppe auszuwählen. Der ausgewählte Benutzer oder die ausgewählte Gruppe wird autorisiert, Berechtigungen für die Stammordner der deprovisionierten Benutzer zu steuern.

Sie können die Richtlinie auch so konfigurieren, dass sie Stammordner löscht. Wenn Sie das Kontrollkästchen **Den Basisordner beim Löschen des Benutzerkontos löschen** aktivieren, löscht Quest One ActiveRoles aufgrund dieser Richtlinie den Stammordner, sobald das ihm zugeordnete Benutzerkonto gelöscht wird. Sie können dieses Verhalten genauer steuern, indem Sie in der Liste unter dem Kontrollkästchen eine der folgenden Optionen auswählen:

- **Wenn Stammordner leer ist.** Verhindert, dass Quest One ActiveRoles nicht leere Stammordner löscht. Wenn ein Stammordner beliebige Daten enthält, löscht die Richtlinie ihn nicht.
- **Immer.** Ermöglicht Quest One ActiveRoles das Löschen leerer und nicht leerer Stammordner. Unabhängig davon, ob ein Stammordner Daten enthält, löscht die Richtlinie ihn bei der Löschung des Benutzerkontos.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Verfahren zum Konfigurieren einer Stammordner-Deprovisionierungsrichtlinie

So konfigurieren Sie eine Richtlinie zur Bereitstellungsrücknahme für Stammordner:

1. Wählen Sie auf der Seite **Zu konfigurierende Richtlinie** die Option **Stammordner-Stilllegung** aus und klicken Sie dann auf **Weiter**.
2. Wählen Sie auf der Seite **Optionen zur Bereitstellungsrücknahme für Basisordner** die Optionen aus, die die Richtlinie anwenden soll, wenn Sie ein Benutzerkonto deprovisionieren. Sie können jede beliebige Kombination dieser Optionen auswählen, um den Stammordner für das deprovisionierte Benutzerkonto zu deprovisionieren.
   - Benutzerberechtigungen für Basisordner entfernen
   - Vorgesetztem des Benutzers schreibgeschützten Zugriff auf den Basisordner gewähren
   - Diesen Benutzern oder Gruppen schreibgeschützten Zugriff auf den Basisordner gewähren
   - Diesen Benutzer oder diese Gruppe zum Eigentümer des Basisordners machen
   - Den Basisordner beim Löschen des Benutzerkontos löschen
3. Wenn Sie das Kontrollkästchen **Diesen Benutzern oder Gruppen schreibgeschützten Zugriff auf den Stammordner gewähren** aktiviert haben, klicken Sie auf **Wählen** und verwenden Sie das Dialogfeld **Objekte auswählen**, um die gewünschten Benutzer oder Gruppen anzugeben.
4. Wenn Sie das Kontrollkästchen **Diesen Benutzer oder diese Gruppe zum Besitzer des Stammordners machen** aktiviert haben, klicken Sie auf **Wählen** und verwenden Sie das Dialogfeld **Objekte auswählen**, um die gewünschten Benutzer oder Gruppen anzugeben.

5. Wenn Sie das Kontrollkästchen **Den Basisordner beim Löschen des Benutzerkontos löschen** aktiviert haben, wählen Sie eine dieser Optionen aus:
   - **Immer**, damit die Richtlinie den Stammordner unabhängig davon, ob der Ordner Dateien oder Unterordner enthält, löscht.
   - **Wenn Stammordner leer ist**, um zu verhindern, dass der Stammordner gelöscht wird, wenn er irgendwelche Dateien oder Unterordner enthält.
6. Klicken Sie auf **Weiter**.
7. Auf der Seite **Richtlinie erzwingen** können Sie Objekte angeben, auf die dieses Richtlinienobjekt angewandt werden soll:
   - Klicken Sie auf **Hinzufügen** und verwenden Sie das Objekt **Objekte auswählen**, um die gewünschten Objekte auszuwählen.
8. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Szenario: Entfernen des Zugriffs auf einen Stammordner

Die in diesem Szenario beschriebene Richtlinie führt während der Deprovisionierung für einen Benutzer die folgenden Funktionen aus:

- Entfernen aller Berechtigungen des Benutzers für den eigenen Stammordner.
- Legt die Administratorengruppe als Besitzer deprovisionierter Stammordner fest.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Bei der Deprovisionierung für ein Benutzerkonto in dem Container, den Sie in Schritt 2 ausgewählt haben, ändert Quest One ActiveRoles folglich die Sicherheit für den Stammordner des Benutzers, wie von dieser Richtlinie vorgeschrieben.

In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten „Neues Deprovisionsrichtlinienobjekt" erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter Erstellen eines Richtlinienobjekts im Abschnitt Verwaltungsaufgaben für Richtlinienobjekte weiter oben in diesem Kapitel.

Um die Richtlinie zu konfigurieren, klicken Sie auf **Stammordner-Deprovisionierung** auf der Seite **Auswählen des Richtlinientyps** des Assistenten. Klicken Sie dann auf **Weiter**.

Aktivieren Sie auf der Seite **Optionen zur Bereitstellungsrücknahme für Basisordner** die folgenden Kontrollkästchen:

- **Benutzerberechtigungen für Basisordner entfernen**
- **Vorgesetztem des Benutzers schreibgeschützten Zugriff auf den Basisordner gewähren**

Stellen sie sicher, dass keine anderen Kontrollkästchen auf der Seite aktiviert sind. Klicken Sie dann auf **Weiter** und befolgen Sie die Anweisungen im Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten für neues Deprovisionsrichtlinienobjekt anwenden, oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen bezüglich der Anwendung eines Richtlinienobjekts finden Sie unter Anwenden von Richtlinienobjekten und Verwalten des Richtlinienbereichs weiter oben in diesem Kapitel.

Benutzerkonto-Verschiebung

Richtlinien dieser Kategorie dienen zum Automatisieren der Verschiebung von deprovisionierten Benutzerkonten in angegebene Organisationseinheiten. So werden solche Konten der Steuerung der Administratoren entzogen, die die Organisationseinheiten verwalten, in denen sich diese Konten ursprünglich befanden. Eine Richtlinie dieser Kategorie kann auch so konfiguriert werden, dass sie deprovisionierte Benutzerkonten nicht verschiebt.

Funktionsweise dieser Richtlinie

Beim Verarbeiten einer Deprovisionsanforderung für einen Benutzer verwendet Quest One ActiveRoles diese Richtlinie, um zu bestimmen, ob das deprovisionierte Benutzerkonto in eine andere Organisationseinheit verschoben werden soll.

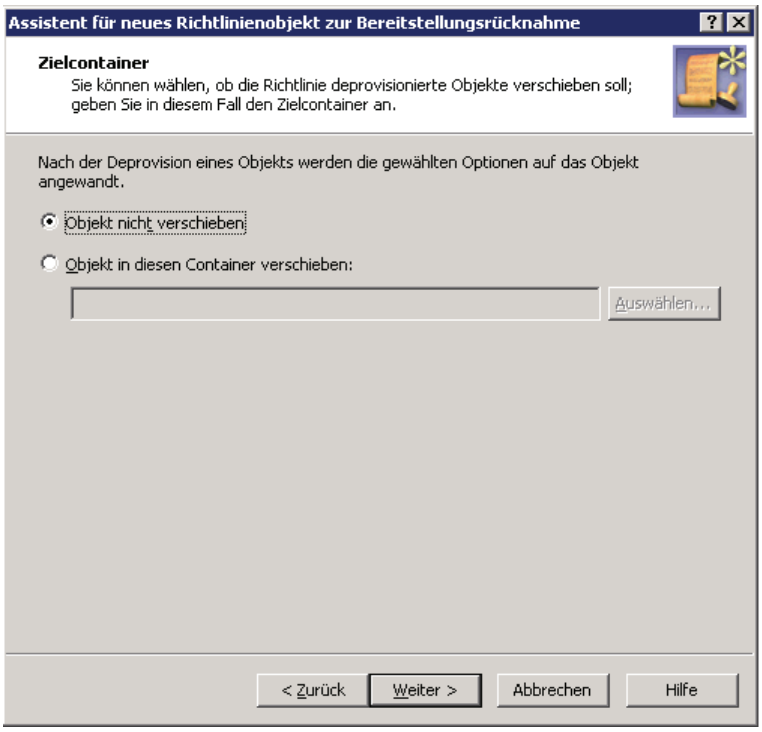
Eine für das Verschieben von Benutzerkonten konfigurierte Richtlinie gibt auch das Ziel an, also die Organisationseinheit, in die Quest One ActiveRoles deprovisionierte Benutzerkonten verschiebt.

Es kann auch eine Richtlinie konfiguriert werden, die Benutzerkonten nicht verschiebt. Wenn eine solche Richtlinie auf einer bestimmten Ebene der Verzeichnishierarchie angewendet wird, setzt sie ggf. alle anderen Richtlinien dieser Kategorie außer Kraft, die auf einer höheren Ebene der Verzeichnishierarchie angewendet werden.

Das folgende Beispiel verdeutlicht dieses Verhalten. Nehmen Sie an, Sie konfigurieren eine Richtlinie für das Verschieben von Konten und wenden sie auf einen bestimmten übergeordneten Container an. Im Allgemeinen wird die Richtlinie vom übergeordneten Container an untergeordnete Container übergeben. Sie wird also auf alle untergeordneten Container des jeweiligen übergeordneten Containers angewendet, und Quest One ActiveRoles verschiebt folglich deprovisionierte Benutzerkonten aus allen diesen Containern. Wenn Sie jedoch eine andere Richtlinie konfigurieren, mit der Konten nicht verschoben werden, und diese neue Richtlinie auf einen untergeordneten Container anwenden, setzt die Richtlinie des untergeordneten Containers die vom übergeordneten Container geerbte Richtlinie außer Kraft. Quest One ActiveRoles verschiebt dann keine deprovisionierten Benutzerkonten aus diesem untergeordneten Container oder den Containern darunter.

Konfigurieren der Richtlinie „Benutzerkonto-Verschiebung“

Um die Richtlinie „Benutzerkonto-Verschiebung“ zu konfigurieren, wählen Sie **Benutzerkonto-Verschiebung** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten „Neues Deprovisionsrichtlinienobjekt“ oder im Assistenten „Deprovisionsrichtlinie hinzufügen“ aus. Klicken Sie dann auf **Weiter**, damit die Seite **Zielcontainer** angezeigt wird.


Assistent für neues Richtlinienobjekt zur Bereitstellungsrücknahme
Zielcontainer
Sie können wählen, ob die Richtlinie deprovisionierte Objekte verschieben soll; geben Sie in diesem Fall den Zielcontainer an.
Nach der Deprovision eines Objekts werden die gewählten Optionen auf das Objekt angewandt.
Objekt nicht verschieben
Objekt in diesen Container verschieben:
Auswählen...
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite können Sie auswählen, ob die Richtlinie deprovisionierte Benutzerkonten verschieben soll, und Sie können den Zielcontainer für den Verschiebungsvorgang auswählen.

Wählen Sie zunächst eine der folgenden Optionen aus:

- Klicken Sie auf **Objekt nicht verschieben**, damit die Richtlinie deprovisionierte Benutzerkonten an ihren ursprünglichen Orten belässt. Mit dieser Option verbleibt jedes deprovisionierte Benutzerkonto in der Organisationseinheit, in der es sich bei der Rücknahme der Bereitstellung befand.
- Klicken Sie auf **Objekt in diesen Container verschieben**, damit die Richtlinie deprovisionierte Benutzerkonten in einen bestimmten Container verschiebt. Mit dieser Option wird jedes deprovisionierte Benutzerkonto von seinem ursprünglichen Ort in eine angegebene Organisationseinheit verschoben.

Für die zweite Option müssen Sie die Organisationseinheit angeben, in die die Richtlinie deprovisionierte Benutzerkonten verschieben soll. Klicken Sie auf die Schaltfläche **Auswählen** und wählen Sie dann die gewünschte Organisationseinheit aus.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Verfahren zum Konfigurieren einer Benutzerkonto-Verschiebungsrichtlinie

So konfigurieren Sie eine Richtlinie zur Benutzerkontoverschiebung:

1. Wählen Sie auf der Seite **Zu konfigurierende Richtlinie** die Option **Benutzerkonto-Verschiebung** aus und klicken Sie dann auf **Weiter**.
2. Führen Sie auf der Seite **Zielcontainer** eine der folgenden Aktionen aus und klicken Sie dann auf **Weiter**:
   - Klicken Sie auf **Objekt nicht verschieben**, wenn die Richtlinie deprovisionierte Benutzerkonten an ihren ursprünglichen Speicherorten belassen soll.
   - Klicken Sie auf **Objekt in diesen Container verschieben**, damit die Richtlinie die deprovisionierten Benutzerkonten in einen bestimmten Container verschiebt. Klicken Sie dann auf **Wählen** und wählen Sie den gewünschten Container aus.
3. Auf der Seite **Richtlinie erzwingen** können Sie Objekte angeben, auf die dieses Richtlinienobjekt angewandt werden soll:
   - Klicken Sie auf **Hinzufügen** und verwenden Sie das Objekt **Objekte auswählen**, um die gewünschten Objekte auszuwählen.
4. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Szenario: Organisationseinheit zum Ablegen deprovisionierter Benutzerkonten

In diesem Szenario wird das Konfigurieren einer Richtlinie beschrieben, die dazu führt, dass eine bestimmte Organisationseinheit alle deprovisionierten Benutzerkonten enthält.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Nach der Deprovisionierung für ein Benutzerkonto in dem Container, den Sie in Schritt 2 ausgewählt haben, verschiebt Quest One ActiveRoles folglich dieses Konto automatisch in die von der Richtlinienkonfiguration bestimmte Organisationseinheit. In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten „Neues Deprovisionsrichtlinienobjekt" erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter Erstellen eines Richtlinienobjekts im Abschnitt Verwaltungsaufgaben für Richtlinienobjekte weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Richtlinientyp auswählen** des Assistenten auf **Benutzerkonto-Verschiebung**. Klicken Sie dann auf **Weiter**.

Klicken Sie auf der Seite **Zielcontainer** auf **Objekt in diesen Container verschieben**. Klicken Sie dann auf die Schaltfläche **Auswählen**, um das Dialogfeld **Container suchen** anzuzeigen. Suchen Sie die Organisationseinheit, in die die Richtlinie deprovisionierte Benutzerkonten verschieben soll, und wählen Sie sie aus. Klicken Sie dann auf **OK**.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten für neues Deprovisionsrichtlinienobjekt anwenden, oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen bezüglich der Anwendung eines Richtlinienobjekts finden Sie unter Anwenden von Richtlinienobjekten und Verwalten des Richtlinienbereichs weiter oben in diesem Kapitel.

Permanentes Löschen des Benutzerkontos

Richtlinien dieser Kategorie dienen zum Automatisieren der Löschung von deprovisionierten Benutzerkonten. Deprovisionierte Benutzerkonten werden für einen angegebenen Zeitraum beibehalten, bevor sie dauerhaft gelöscht werden. Eine Richtlinie dieser Kategorie kann auch so konfiguriert werden, dass sie deprovisionierte Konten nicht löscht.

Funktionsweise dieser Richtlinie

Beim Verarbeiten einer Deprovisionsanforderung für einen Benutzer verwendet Quest One ActiveRoles diese Richtlinie, um zu bestimmen, ob für das deprovisionierte Benutzerkonto die Löschung geplant werden soll. Ein Benutzerkonto, für das die Löschung geplant ist, wird nach einem bestimmten Zeitraum dauerhaft gelöscht. Dieser wird als *Wartezeitraum* bezeichnet.

Eine Richtlinie, die zum Löschen von Benutzerkonten konfiguriert ist, gibt an, für wie viele Tage deprovisionierte Benutzerkonten beibehalten werden sollen. Mit einer solchen Richtlinie löscht Quest One ActiveRoles ein Benutzerkonto nach der angegebenen Anzahl von Tagen seit der Deprovisionierung für den Benutzer dauerhaft.

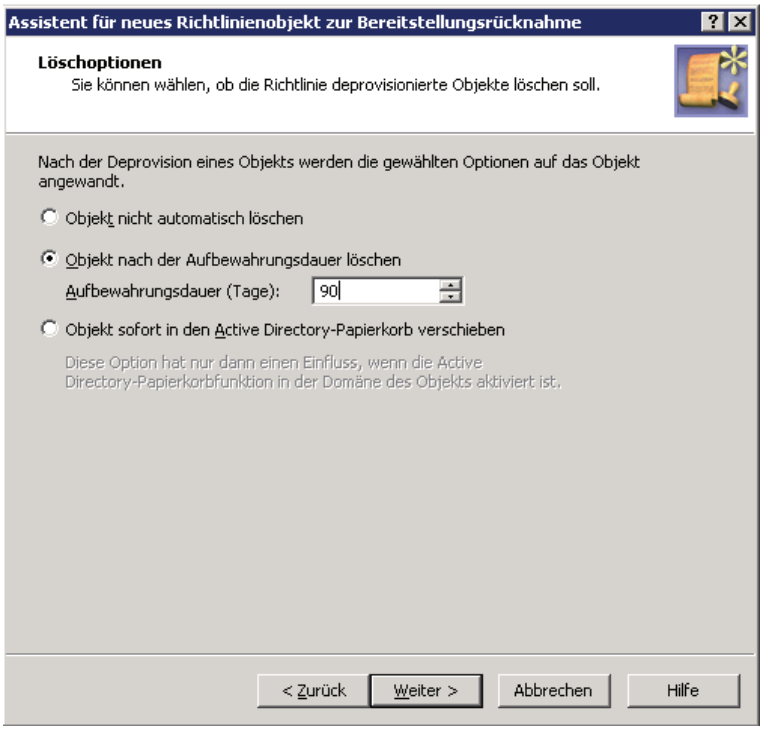
Es kann auch eine Richtlinie konfiguriert werden, die Benutzerkonten nicht löscht. Wenn eine solche Richtlinie auf einer bestimmten Ebene der Verzeichnishierarchie angewendet wird, setzt sie ggf. alle anderen Richtlinien dieser Kategorie außer Kraft, die auf einer höheren Ebene der Verzeichnishierarchie angewendet werden.

Das folgende Beispiel verdeutlicht dieses Verhalten. Nehmen Sie an, Sie konfigurieren eine Richtlinie für das Löschen von Konten und wenden sie auf einen bestimmten Container an. Im Allgemeinen wird die Richtlinie vom übergeordneten Container an untergeordnete Container übergeben. Sie wird also auf alle untergeordneten Container des jeweiligen übergeordneten Containers angewendet, und Quest One ActiveRoles löscht folglich deprovisionierte Benutzerkonten aus allen diesen Containern. Wenn Sie jedoch eine andere Richtlinie konfigurieren, mit der Konten nicht gelöscht werden, und diese neue Richtlinie auf einen untergeordneten Container anwenden, setzt die Richtlinie des untergeordneten Containers die vom übergeordneten Container geerbte Richtlinie außer Kraft. Quest One ActiveRoles löscht dann keine deprovisionierten Benutzerkonten aus diesem untergeordneten Container oder den Containern darunter.

Eine weitere Option dieser Richtlinie gilt für Domänen, in denen die Active Directory-Papierkorbfunktion aktiviert ist. Die Richtlinie kann so konfiguriert werden, dass ein Benutzerkonto direkt nach seiner Deprovisionierung in den Papierkorb verschoben wird (was bedeutet, dass das Konto sofort und ohne jegliche Aufbewahrungsdauer gelöscht wird). Das Verschieben von deprovisionierten Benutzerkonten in den Papierkorb kann aus Sicherheitsgründen als zusätzliche Maßnahme erforderlich sein. Der Active Directory-Papierkorb gewährleistet, dass das Konto bei Bedarf ohne jeglichen Datenverlust wiederhergestellt werden kann. Quest One ActiveRoles bietet die Möglichkeit, das Löschen von Benutzerkonten, die in den Papierkorb deprovisioniert wurden, rückgängig zu machen und die Deprovisionierung dann aufzuheben.

Konfigurieren der Richtlinie „Permanentes Löschen von Benutzerkonten“

Um eine Richtlinie bezüglich des permanenten Löschens von Benutzerkonto zu konfigurieren, wählen Sie **Permanentes Löschen des Benutzerkontos** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten „Neues Deprovisionsrichtlinienobjekt“ oder im Assistenten „Deprovisionsrichtlinie hinzufügen“ aus. Klicken Sie dann auf **Weiter**, damit die Seite **Löschoptionen** angezeigt wird.


Assistent für neues Richtlinienobjekt zur Bereitstellungsrücknahme
Löschoptionen
Sie können wählen, ob die Richtlinie deprovisionierte Objekte löschen soll.
Nach der Deprovision eines Objekts werden die gewählten Optionen auf das Objekt angewandt.
Objekt nicht automatisch löschen
Objekt nach der Aufbewahrungsdauer löschen
Aufbewahrungsdauer (Tage):
90
Objekt sofort in den Active Directory-Papierkorb verschieben
Diese Option hat nur dann einen Einfluss, wenn die Active Directory-Papierkorbfunktion in der Domäne des Objekts aktiviert ist.
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite können Sie auswählen, ob die Richtlinie für deprovisionierte Benutzerkonten die Löschung planen soll. Außerdem können Sie angeben, für wie viele Tage deprovisionierte Benutzerkonten beibehalten werden sollen.

Wählen Sie zunächst eine der folgenden Optionen aus:

- Klicken Sie auf **Objekt nicht automatisch löschen**, damit die Richtlinie deprovisionierte Benutzerkonten nicht löscht.
- Klicken Sie auf **Objekt nach der Aufbewahrungsdauer löschen**, damit die Richtlinie für deprovisionierte Benutzerkonten die Löschung plant.
- Klicken Sie auf **Objekt sofort in den Active Directory-Papierkorb verschieben**, damit die Richtlinie die deprovisionierten Benutzerkonten in einen bestimmten Container verschiebt.

Wenn Sie die zweite Option auswählen, müssen Sie in dem Feld unter dieser Option eine Anzahl von Tagen angeben. Nachdem ein Benutzerkonto deprovisioniert wurde und die angegebene Anzahl von Tagen vergangen ist, löscht Quest One ActiveRoles aufgrund der Richtlinie das Benutzerkonto aus Active Directory.

Wenn Sie die dritte Option auswählen, sollten Sie diese Richtlinie auf Domänen anwenden, in denen der Active Directory-Papierkorb aktiviert ist; andernfalls hat die Richtlinie keine Auswirkungen. Bei Aktivierung dieser Option führt die Richtlinie, sobald ein Benutzerkonto deprovisioniert wurde, dazu, dass Quest One ActiveRoles das Benutzerkonto sofort löscht. In einer Domäne, in der der Active Directory-Papierkorb aktiviert ist, bedeutet dieser Löschvorgang bloß, dass das Konto als gelöscht markiert und in einen bestimmten Container verschoben wird, aus dem es bei Bedarf ohne Datenverlust wiederhergestellt werden kann.

Verfahren zum Konfigurieren einer Richtlinie bezüglich des permanenten Löschens eines Benutzerkontos

So konfigurieren Sie eine Richtlinie zur dauerhaften Löschung von Benutzerkonten:

1. Wählen Sie auf der Seite **Zu konfigurierende Richtlinie** die Option **Permanentes Löschen von Benutzerkonto** aus und klicken Sie dann auf **Weiter**.
2. Führen Sie auf der Seite **Löschoptionen** eine der folgenden Aktionen aus und klicken Sie dann auf **Weiter**:
   - Klicken Sie auf **Objekt nicht automatisch löschen**, damit die Richtlinie deprovisionierte Benutzerkonten nicht löscht.
   - Klicken Sie auf **Objekt nach der Aufbewahrungsdauer löschen**, damit die Richtlinie für deprovisionierte Benutzerkonten die Löschung plant. Geben Sie dann unter **Aufbewahrungsdauer (Tage)** die Anzahl der Tage an, wie lange das deprovisionierte Benutzerkonto beibehalten werden soll, bevor es gelöscht wird.
   - Klicken Sie auf **Objekt sofort in den Active Directory-Papierkorb verschieben**, damit die Richtlinie die deprovisionierten Benutzerkonten in einen bestimmten Container verschiebt.

   Wenn Sie die dritte Option auswählen, sollten Sie diese Richtlinie auf Domänen anwenden, in denen der Active Directory-Papierkorb aktiviert ist; andernfalls hat die Richtlinie keine Auswirkungen. Bei Aktivierung dieser Option führt die Richtlinie, sobald ein Benutzerkonto deprovisioniert wurde, dazu, dass Quest One ActiveRoles das Benutzerkonto sofort löscht. In einer Domäne, in der der Active Directory-Papierkorb aktiviert ist, bedeutet dieser Löschvorgang bloß, dass das Konto als gelöscht markiert und in einen bestimmten Container verschoben wird, aus dem es bei Bedarf ohne Datenverlust wiederhergestellt werden kann.
3. Im Fenster **Richtlinie erzwingen** können Sie Objekte angeben, auf die dieses Richtlinienobjekt angewandt werden soll:
   - Klicken Sie auf **Hinzufügen** und verwenden Sie das Objekt **Objekte auswählen**, um die gewünschten Objekte auszuwählen.
4. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Szenario: Löschen deprovisionierter Benutzerkonten

In diesem Szenario wird beschrieben, wie Sie eine Richtlinie konfigurieren, damit Quest One ActiveRoles deprovisionierte Benutzerkonten nach einem Wartezeitraum von 90 Tagen dauerhaft löscht.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Nach der Deprovisionierung für ein Benutzerkonto in dem Container, den Sie in Schritt 2 ausgewählt haben, behält Quest One ActiveRoles folglich dieses Konto für 90 Tage bei und löscht es dann.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten „Neues Deprovisionsrichtlinienobjekt" erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter Erstellen eines Richtlinienobjekts im Abschnitt Verwaltungsaufgaben für Richtlinienobjekte weiter oben in diesem Kapitel.

Um die Richtlinie zu konfigurieren, klicken Sie auf **Permanentes Löschen des Benutzerkontos** auf der Seite **Auswählen des Richtlinientyps** des Assistenten. Klicken Sie dann auf **Weiter**.

Klicken Sie auf der Seite **Löschoptionen** auf **Objekt nach Wartezeitraum löschen**. Geben Sie dann in das Feld unter dieser Option den Wert **90** ein.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten für neues Deprovisionsrichtlinienobjekt anwenden, oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen bezüglich der Anwendung eines Richtlinienobjekts finden Sie unter Anwenden von Richtlinienobjekten und Verwalten des Richtlinienbereichs weiter oben in diesem Kapitel.

Gruppenobjekt-Deprovisionierung

Die Richtlinie zur Deprovisionierung von Gruppenobjekten gibt die Änderungen an, die am Gruppenobjekt in Active Directory vorzunehmen sind, um die Verwendung der Gruppe zu vermeiden. Sie dient zur Durchführung der folgenden Aufgaben im Rahmen der Deprovisionierung einer Gruppe:

- Gruppe in der globalen Adressliste (GAL) ausblenden, um den Zugriff auf die Gruppe ausgehend von Exchange Server-Client-Anwendungen wie etwa Microsoft Outlook zu verhindern.
- Ändern des Typs der Gruppe von „Sicherheit" in „Verteilung", um die Zugriffsrechte von dieser Gruppe zurückzuziehen.
- Umbenennen der Gruppe, um deprovisionierte Gruppen nach Namen unterscheiden zu können.
- Entfernen von Mitgliedern aus dieser Gruppe, um den Benutzerzugriff auf Ressourcen zu widerrufen, die von der Gruppe kontrolliert werden. Diese Aufgabe bietet die Möglichkeit zur Angabe der Mitglieder, die nicht aus der Gruppe entfernt werden sollen.

Darüber hinaus kann die Richtlinie so konfiguriert werden, dass sie jegliche andere Eigenschaften einer Gruppe wie etwa den Prä-Windows 2000-Namen, E-Mail-Adressen oder die Beschreibung ändert oder löscht.

Funktionsweise dieser Richtlinie

Beim Verarbeiten einer Deprovisionsanforderung für eine Gruppe verwendet Quest One ActiveRoles diese Richtlinie, um das Gruppenobjekt in Active Directory so zu ändern, dass die Gruppe nach ihrer Deprovisionierung nicht mehr verwendet werden kann.

Es kann auch eine Richtlinie zum Aktualisieren einzelner Eigenschaften der Gruppen konfiguriert werden. Abhängig von der Richtlinienkonfiguration hat jede richtlinienbasierte Aktualisierung folgende Ergebnisse:

- Bestimmte Abschnitte der Gruppeninformationen wie etwa die Informationen über Gruppenmitglieder werden aus dem Verzeichnis entfernt.
- Bestimmte Eigenschaften von Gruppen werden geändert oder gelöscht.

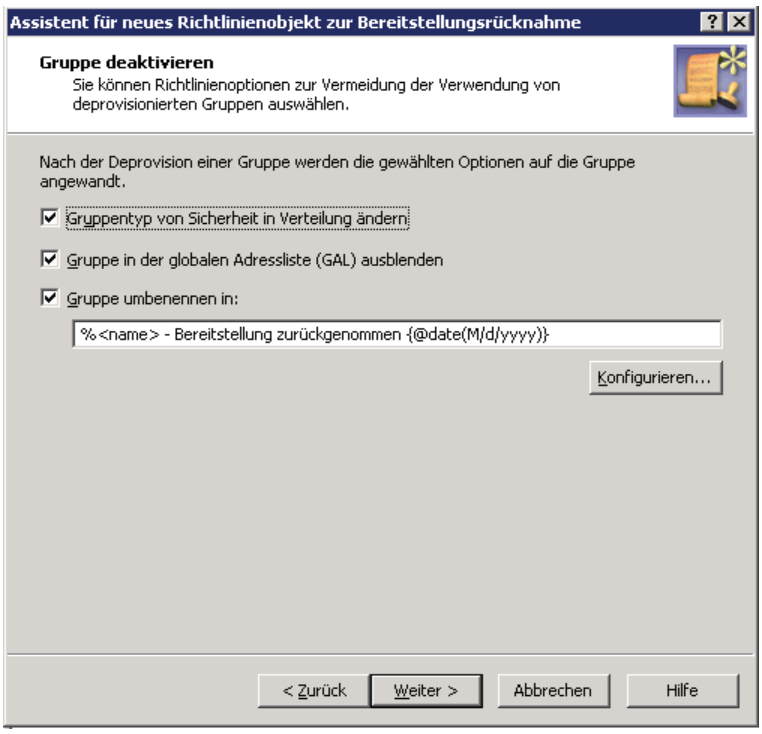
Eine Richtlinie kann so konfiguriert werden, dass sie folgende neue Eigenschaftswerte einschließt:

- Eigenschaften der Gruppe, für die die Bereitstellung zurückgenommen wird. Diese Eigenschaften wurden vor dem Beginn des Rücknahmevorgangs für die Gruppe aus dem Verzeichnis abgerufen
- Eigenschaften des Benutzers, der die Anfrage zur Deprovisionierung gestellt hat
- Datum und Uhrzeit der Deprovisionierung der Gruppe

Quest One ActiveRoles ändert also bei der Deprovisionierung einer Gruppe das Gruppenobjekt in Active Directory so, wie es von der gültigen Richtlinie zur Deprovisionierung von Gruppenobjekten bestimmt wird.

Konfigurieren der Gruppenobjekt-Deprovisionierungsrichtlinie

Um die Gruppenobjekt-Deprovisionierungsrichtlinie zu konfigurieren, wählen Sie **Gruppenobjekt-Deprovisionierung** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten „Neues Deprovisionsrichtlinienobjekt" oder im Assistenten „Deprovisionsrichtlinie hinzufügen" aus. Klicken Sie dann auf **Weiter**, damit die Seite **Gruppe deaktivieren** angezeigt wird.


Assistent für neues Richtlinienobjekt zur Bereitstellungsrücknahme
Gruppe deaktivieren
Sie können Richtlinienoptionen zur Vermeidung der Verwendung von deprovisionierten Gruppen auswählen.
Nach der Deprovision einer Gruppe werden die gewählten Optionen auf die Gruppe angewandt.
Gruppentyp von Sicherheit in Verteilung ändern
Gruppe in der globalen Adressliste (GAL) ausblenden
Gruppe umbenennen in:
%<name> - Bereitstellung zurückgenommen {@date(M/d/yyyy)}
Konfigurieren...
< Zurück
Weiter >
Abbrechen
Hilfe

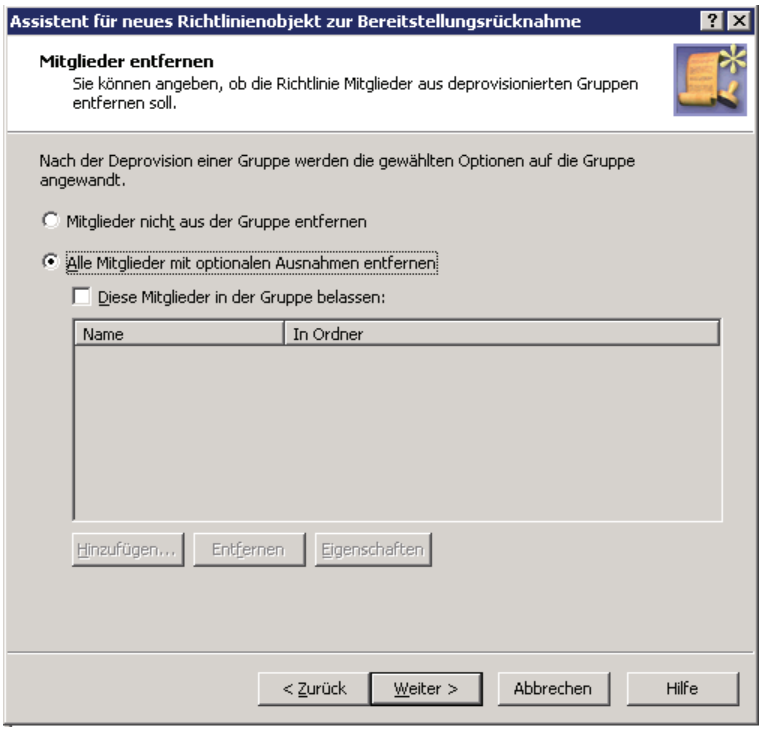
Auf dieser Seite können Sie unter den folgenden Optionen wählen:

- **Gruppentyp von Sicherheit in Verteilung ändern.** Widerruft Zugriffsrechte von deprovisionierten Gruppen. Diese Option gilt nur für Sicherheitsgruppen.
- **Gruppe in der globalen Adressliste (GAL) ausblenden.** Verhindert den Zugriff auf deprovisionierte Gruppen ausgehend von Exchange Server-Client-Anwendungen. Diese Option ist auf Verteilergruppen oder E-Mail-fähige Sicherheitsgruppen anwendbar.
- **Gruppe umbenennen in.** Ändert den Namen der Gruppe.

Aktivieren Sie das Kontrollkästchen neben jeder Option, auf die die Richtlinie angewandt werden soll.

Durch Aktivieren des Kontrollkästchens **Gruppe umbenennen in** weisen Sie die Richtlinie an, den Namen der Gruppe zu ändern. Mit dieser Option können Sie eine *Eigenschaftsaktualisierungsregel* konfigurieren, die angibt, wie der Gruppenname geändert werden soll. Klicken Sie auf die Schaltfläche **Konfigurieren** und folgen Sie den Anweisungen im Abschnitt Dabei wird der Benutzername als Beispiel verwendet. weiter oben in diesem Kapitel.

Wenn Sie die Seite **Gruppe deaktivieren** abgeschlossen haben, klicken Sie auf **Weiter**, um die Seite **Mitglieder entfernen** anzuzeigen:


Assistent für neues Richtlinienobjekt zur Bereitstellungsrücknahme
Mitglieder entfernen
Sie können angeben, ob die Richtlinie Mitglieder aus deprovisionierten Gruppen entfernen soll.
Nach der Deprovision einer Gruppe werden die gewählten Optionen auf die Gruppe angewandt.
Mitglieder nicht aus der Gruppe entfernen
Alle Mitglieder mit optionalen Ausnahmen entfernen
Diese Mitglieder in der Gruppe belassen:
Name
In Ordner
Hinzufügen...
Entfernen
Eigenschaften
< Zurück
Weiter >
Abbrechen
Hilfe

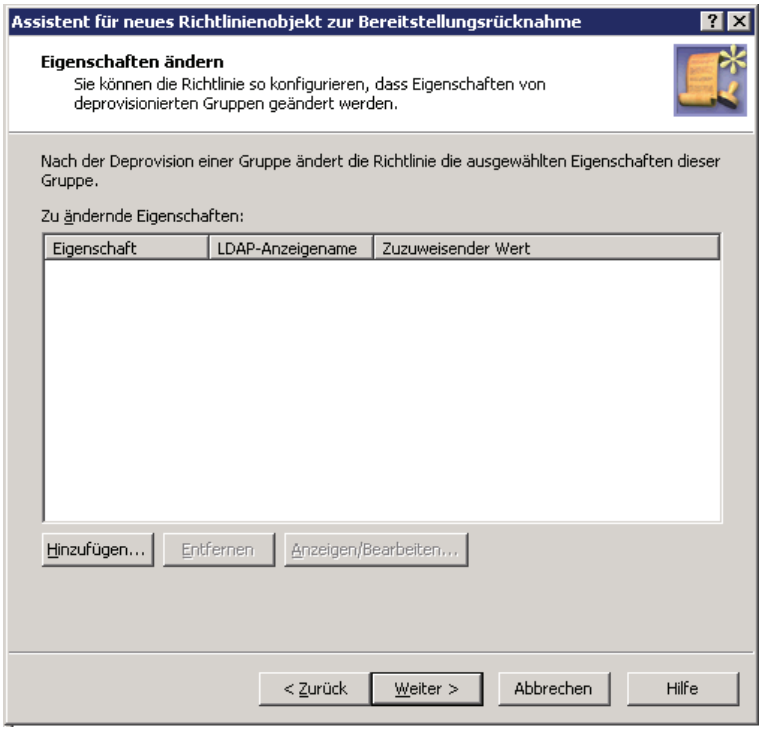
Auf dieser Seite können Sie eine Regel konfigurieren, die angibt, wie Mitglieder aus deprovisionierten Gruppen entfernt werden sollen.

Wählen Sie eine der folgenden Optionen aus:

- Klicken Sie auf **Mitglieder nicht aus der Gruppe entfernen**, wenn Sie möchten, dass die Richtlinie keine Mitglieder aus deprovisionierten Gruppen entfernt.
- Klicken Sie auf **Alle Mitglieder mit optionalen Ausnahmen entfernen**, wenn Sie möchten, dass die Richtlinie Mitglieder aus deprovisionierten Gruppen entfernt.

Mit der zweiten Option können Sie angeben, ob die Richtlinie bestimmte Objekte aus deprovisionierten Gruppen nicht entfernen soll. Um eine Liste solcher Objekte einzurichten, aktivieren Sie das Kontrollkästchen **Diese Mitglieder in der Gruppe belassen**, klicken Sie dann auf die Schaltfläche **Hinzufügen** und wählen Sie die Objekte aus, die Sie in die Liste einschließen möchten.

Wenn Sie die Seite **Mitglieder entfernen** abgeschlossen haben, klicken Sie auf **Weiter**, um die Seite **Eigenschaften ändern** anzuzeigen:



Auf dieser Seite können Sie eine Liste von Gruppeneigenschaften einrichten, die die Richtlinie aktualisieren soll. Jeder Eintrag in der Liste schließt die folgenden Informationen ein:

- **Eigenschaft.** Bei der Deprovisionierung einer Gruppe aktualisiert Quest One ActiveRoles diese Eigenschaft des Gruppenobjekts in Active Directory.
- **LDAP-Anzeigename.** Identifiziert die zu aktualisierende Eigenschaft eindeutig.
- **Zuzuweisender Wert.** Nach dem Abschluss des Deprovisionierungsvorgangs besitzt die Eigenschaft den durch die angegebene Regel definierten Wert.

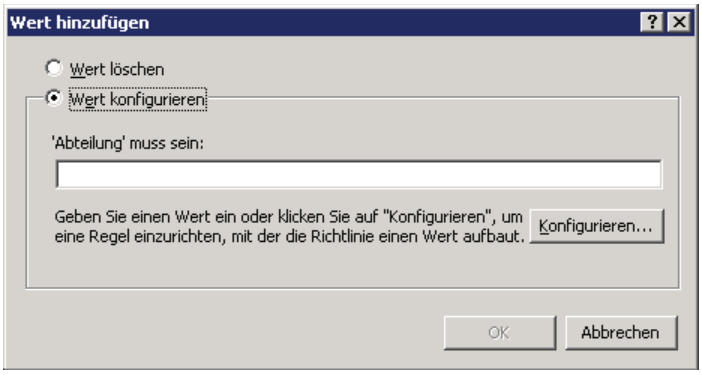
Sie können die Liste auf dieser Seite mit folgenden Schaltflächen verwalten:

- **Hinzufügen.** Ermöglicht das Auswählen einer Eigenschaft und das Konfigurieren einer Aktualisierungsregel für diese Eigenschaft. Eine Eigenschaftsaktualisierungsregel gibt an, wie der neue Wert generiert werden soll, der der Eigenschaft zugewiesen wird.
- **Entfernen.** Wenn die Richtlinie eine bestimmte Eigenschaft nicht mehr aktualisieren soll, wählen Sie die Eigenschaft in der Liste aus und klicken Sie auf **Entfernen**.
- **Anzeigen/Bearbeiten.** Ermöglicht das Ändern der Aktualisierungsregel für die Eigenschaft, die Sie in der Liste auswählen.

Wenn Sie auf die Schaltfläche **Hinzufügen** klicken, wird das Dialogfeld **Objekteigenschaft wählen** angezeigt. In diesem können Sie Gruppeneigenschaften auswählen, die die Richtlinie aktualisieren soll. Um eine Eigenschaft auszuwählen, aktivieren Sie das Kontrollkästchen neben dem Eigenschaftsnamen und klicken Sie dann auf **OK**.

Sie können mehrere Kontrollkästchen aktivieren. In diesem Fall werden die ausgewählten Eigenschaften der Liste auf der Seite des Assistenten hinzugefügt, und die Aktualisierungsregel wird so konfiguriert, dass sie diese Eigenschaften löscht, ihnen also den „leeren" Wert zuweist.

Wenn Sie eine einzelne Eigenschaft im Dialogfeld **Objekteigenschaft wählen** auswählen, wird das Dialogfeld **Wert hinzufügen** angezeigt, sodass Sie den Vorgang mit der Konfiguration einer Eigenschafts-Aktualisierungsregel fortsetzen können:


Wert hinzufügen
Wert löschen
Wert konfigurieren
'Abteilung' muss sein:
Geben Sie einen Wert ein oder klicken Sie auf "Konfigurieren", um eine Regel einzurichten, mit der die Richtlinie einen Wert aufbaut.
Konfigurieren...
OK
Abbrechen

Sie können eine der folgenden Aktualisierungsoptionen auswählen:

- **Wert löschen.** Veranlasst die Richtlinie dazu, der Eigenschaft den „leeren" Wert zuzuweisen.
- **Wert konfigurieren.** Ermöglicht das Konfigurieren eines Wertes für die Bedingung **'Eigenschaft' muss sein**.

Bei der zweiten Option müssen Sie einen Wert konfigurieren, den die Richtlinie bei der Deprovisionierung einer Gruppe der Eigenschaft zuweisen soll. Sie können einen Wert auf die gleiche Weise konfigurieren wie beim Konfigurieren einer Eigenschaftsaktualisierungsregel für den Benutzernamen: Klicken Sie auf die Schaltfläche **Konfigurieren** und folgen Sie den Anweisungen im Abschnitt Dabei wird der Benutzername als Beispiel verwendet. weiter oben in diesem Kapitel.

Klicken Sie nach dem Konfigurieren eines Wertes auf **OK**, um das Dialogfeld **Wert hinzufügen** zu schließen. Der Eigenschaftsname wird zusammen mit der Eigenschaftsaktualisierungsregel der Seite des Assistenten hinzugefügt. Nötigenfalls können Sie die Aktualisierungsregel ändern, indem Sie unter der Eigenschaftenliste auf die Schaltfläche **Anzeigen/Bearbeiten** klicken. Dann wird ein Dialogfeld angezeigt, das dem Dialogfeld **Wert hinzufügen** ähnelt und in dem Sie eine andere Aktualisierungsoption auswählen oder einen anderen Wert für die Bedingung **'Eigenschaft' muss sein** festlegen können.

Klicken Sie nach dem Einrichten der Liste auf der Seite des Assistenten auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Verfahren zum Konfigurieren einer Gruppenobjekt-Deprovisionierungsrichtlinie

So konfigurieren Sie eine Richtlinie zur Deprovisionierung von Gruppenobjekten:

1. Wählen Sie auf der Seite **Zu konfigurierende Richtlinie** die Option **Gruppenobjekt-Deprovisionierung** aus und klicken Sie dann auf **Weiter.**
2. Wählen Sie auf der Seite **Gruppe deaktivieren** die Optionen aus, die die Richtlinie bei der Deprovisionierung einer Gruppe anwenden soll. Sie können jegliche Kombination dieser Optionen auswählen, um die Verwendung der Gruppe zu verhindern:
   - Gruppentyp von „Sicherheit" in „Verteilung" ändern
   - Gruppe in der globalen Adressliste (GAL) ausblenden
   - Gruppe umbenennen
3. Wenn Sie **Gruppe umbenennen in** ausgewählt haben, klicken Sie auf **Konfigurieren** und füllen Sie dann das Dialogfeld **Wert konfigurieren** aus, indem Sie das weiter unten in diesem Thema beschriebene Verfahren ausführen, um festzulegen, wie die Richtlinie den Gruppennamen bei der Deprovisionierung einer Gruppe aktualisiert.
4. Klicken Sie auf **Weiter**.
5. Führen Sie auf der **Seite Mitglieder** entfernen eine der folgenden Operationen aus:
   - Klicken Sie auf **Mitglieder nicht aus der Gruppe entfernen** damit die Richtlinie keine Änderungen an der Mitgliedschaftsliste der Gruppe vornimmt.
   - Klicken Sie auf **Alle Mitglieder mit optionalen Ausnahmen entfernen**, damit die Richtlinie die Mitglieder aus der Gruppe entfernt.
6. Wenn Sie die zweite Option in Schritt 5 ausgewählt haben, geben Sie an, ob die Richtlinie bestimmte Objekte nicht aus deprovisionierten Gruppen entfernen soll. Gehen Sie wie folgt vor:
   - Aktivieren Sie das Kontrollkästchen **Diese Mitglieder in der Gruppe belassen** und erstellen Sie eine Liste der Objekte, die die Richtlinie nicht aus deprovisionierten Gruppen entfernen soll.
   - Wenn die Richtlinie alle Mitglieder aus deprovisionierten Gruppen entfernen soll, lassen Sie das Kontrollkästchen deaktiviert.
7. Geben Sie auf der Seite **Eigenschaften ändern** an, wie die Richtlinie die Eigenschaften des Gruppenobjekts bei der Deprovisionierung einer Gruppe aktualisieren soll:
   - Klicken Sie auf **Hinzufügen** und füllen Sie dann das Dialogfeld **Objekteigenschaft wählen** aus, indem Sie das weiter unten in diesem Thema beschriebene Verfahren befolgen, um Eigenschafts-Aktualisierungsregeln hinzuzufügen.
   - Verwenden Sie **Ansicht/Bearbeiten**, um vorhandene Regeln zu ändern.
   - Verwenden Sie **Entfernen**, um vorhandene Regeln zu löschen.
8. Klicken Sie auf **Weiter**.
9. Auf der Seite **Richtlinie erzwingen** können Sie Objekte angeben, auf die dieses Richtlinienobjekt angewandt werden soll:
   - Klicken Sie auf **Hinzufügen** und verwenden Sie das Objekt **Objekte auswählen**, um die gewünschten Objekte auszuwählen.
10. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Gehen Sie folgendermaßen vor, um das Dialogfeld „Wert konfigurieren" abzuschließen:

1. Klicken Sie auf **Hinzufügen**.
2. Konfigurieren Sie einen Eintrag, in den der Wert aufgenommen werden soll (Anweisungen finden Sie unter Verfahren zum Konfigurieren von Einträgen).
3. Im Dialogfeld **Wert konfigurieren** fügen Sie Einträge hinzu, löschen oder bearbeiten vorhandene Einträge und klicken dann auf **OK**.

Gehen Sie folgendermaßen vor, um das Dialogfeld „Objekteigenschaft auswählen" abzuschließen:

1. Wählen Sie in der Liste **Objekteigenschaft** eine Objekteigenschaft aus und klicken Sie dann auf **OK**. Das Dialogfeld **Wert hinzufügen** wird angezeigt.

   *Wenn Sie mehrere Eigenschaften auswählen, wird das Dialogfeld **Wert hinzufügen** nicht angezeigt. Die Eigenschaften, die Sie ausgewählt haben, werden zur Liste auf der Seite **Eigenschaften ändern** hinzugefügt, und die Aktualisierungsregel wird so konfiguriert, dass sie diese Eigenschaften löscht, ihnen also den „leeren" Wert zuweist.*

2. Führen Sie im Dialogfeld **Wert hinzufügen** eine der folgenden Aktionen durch:
   - Wählen Sie **Wert löschen**, wenn die Aktualisierungsregel der Eigenschaft den Wert „leer" zuordnen soll.
   - Wählen Sie **Wert konfigurieren**, wenn die Aktualisierungsregel der Eigenschaft einen bestimmten, nicht leeren Wert zuordnen soll. Klicken Sie dann auf **Konfigurieren** und vervollständigen Sie das Dialogfeld **Wert konfigurieren** anhand der weiter oben in diesem Thema aufgeführten Verfahrensweise.

Szenario 1: Deaktivieren und Umbenennen von Gruppen bei der Deprovisionierung der Gruppe

Die in diesem Szenario beschriebene Richtlinie führt während der Deprovisionierung für eine Gruppe die folgenden Funktionen aus:

- Bei der Deprovisionierung einer Sicherheitsgruppe Änderung des Gruppentyps in „Verteilung".
- Bei der Deprovisionierung einer Verteilergruppe Entfernung der Gruppe aus der Globalen Adressliste.
- Anhängen des folgenden Suffix an den Gruppennamen: **- Deprovisioniert**, gefolgt von dem Datum, an dem die Gruppe deprovisioniert wurde.

Beispielsweise ändert die Richtlinie den Gruppennamen von **Partner Marketing** in **Partner Marketing – Deprovisioniert am 12/11/2009 um**.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Bei der Deprovisionierung einer Gruppe in dem Container, den Sie in Schritt 2 ausgewählt haben, deaktiviert Quest One ActiveRoles folglich die Gruppe und benennt sie wie von dieser Richtlinie vorgeschrieben um.

In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten „Neues Deprovisionsrichtlinienobjekt" erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter Erstellen eines Richtlinienobjekts im Abschnitt Verwaltungsaufgaben für Richtlinienobjekte weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Richtlinientyp auswählen** des Assistenten auf **Gruppenobjekt-Deprovisionierung**. Klicken Sie dann auf **Weiter**.

Aktivieren Sie auf der Seite **Gruppe deaktivieren** die folgenden Kontrollkästchen:

- **Gruppentyp von „Sicherheit" in „Verteilung" ändern**
- **Gruppe in der globalen Adressliste (GAL) ausblenden**
- **Gruppe umbenennen in**

Geben Sie dann den folgenden Text in das Feld unter der Option **Gruppe umbenennen** in ein:

```
%<name> - Deprovisioned {@date(M/d/yyyy)}
```

Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten für neues Deprovisionsrichtlinienobjekt anwenden, oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen bezüglich der Anwendung eines Richtlinienobjekts finden Sie unter Anwenden von Richtlinienobjekten und Verwalten des Richtlinienbereichs weiter oben in diesem Kapitel.

Szenario 2: Verwaltete Einheit zum Ablegen deprovisionierter Gruppen

In diesem Szenario wird beschrieben, wie Sie eine verwaltete Einheit und eine Gruppenobjekt-Deprovisionierungsrichtlinie so konfigurieren, dass die verwaltete Einheit alle deprovisionierten Gruppen enthält. Die Richtlinie setzt bei der Deprovisionierung einer Gruppe die Eigenschaft **Hinweise** auf **Deprovisioniert**. Die verwaltete Einheit wiederum ist so konfiguriert, dass sie die Gruppen einschließt, deren Eigenschaft **Hinweise** auf **Deprovisioniert** gesetzt ist.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie die verwaltete Einheit.
2. Konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
3. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Nach der Deprovisionierung für eine Gruppe in dem Container, den Sie in Schritt 3 ausgewählt haben, fügt Quest One ActiveRoles folglich diese Gruppe automatisch der in Schritt 1 erstellten verwalteten Einheit hinzu.

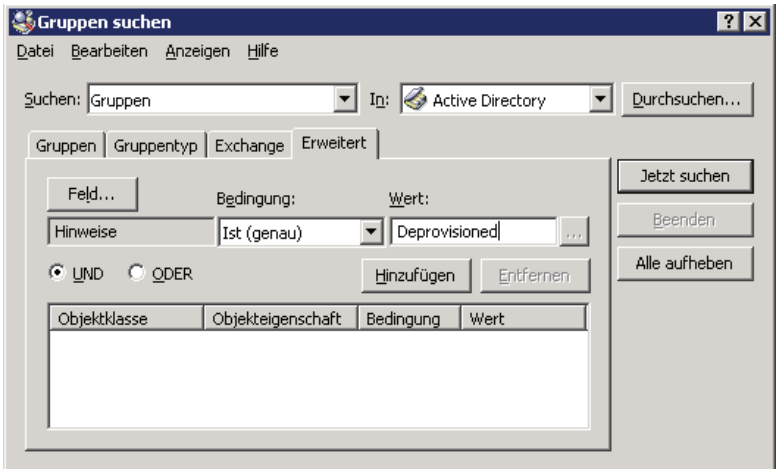
In den folgenden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren der verwalteten Einheit

Sie können die verwaltete Einheit mittels der Quest One ActiveRoles-Konsole erstellen und konfigurieren:

1. Klicken Sie in der Konsolenstruktur unter **Configuration** Klicken Sie mit der rechten Maustaste auf **Verwaltete Einheiten** und wählen Sie **Neu | Verwaltete Einheit**.
2. Geben Sie in das Feld **Name** einen Namen für die verwaltete Einheit ein. Sie können beispielsweise **Deprovisionierte Gruppen** eingeben.
3. Klicken Sie auf **Weiter**.
4. Konfigurieren Sie wie folgt die Mitgliedschaftsregel so, dass die verwaltete Einheit die deprovisionierten Gruppenobjekte aus allen bei Quest One ActiveRoles registrierten Domänen (den verwalteten Domänen) enthält:
   a) Klicken Sie auf der Seite des Assistenten auf **Hinzufügen**.
   b) Klicken Sie im Dialogfeld **Mitgliedschaftsregeltyp** auf **Nach Abfrage einschließen** und klicken Sie dann auf **OK**.
   c) Richten Sie im Fenster **Mitgliedschaftsregel erstellen** die Regel ein:
      - Klicken Sie unter **Suchen** auf **Gruppen**.
      - Klicken Sie auf **Durchsuchen** und wählen Sie **Active Directory**.
      - Klicken Sie auf die Registerkarte **Erweitert**.
      - Klicken Sie auf die Schaltfläche **Feld** und dann auf **Hinweise**.
      - Klicken Sie unter **Bedingung** auf **Ist (genau)**.
      - Geben Sie unter **Wert** den Wert **Deprovisioniert** ein.

   Nun sollte das Fenster der folgenden Abbildung entsprechen:



   - Klicken Sie auf die Schaltfläche **Hinzufügen**.
   - Klicken Sie auf die Schaltfläche **Regel hinzufügen**.

   d) Klicken Sie auf der Seite des Assistenten auf **Hinzufügen**.
   e) Klicken Sie im Dialogfeld **Mitgliedschaftsregeltyp** auf **Deprovisionierte beibehalten** und klicken Sie dann auf **OK**.
5. Klicken Sie auf **Weiter**, wiederum auf **Weiter** und dann auf **Fertig stellen**.

Schritt 2: Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt konfigurieren, indem Sie das Richtlinienobjekt ändern, das das vorige Szenario implementiert; siehe „Szenario 1: Deaktivieren und Umbenennen von Gruppen bei der Gruppendeprovisionierung" weiter oben in diesem Abschnitt.

Zeigen Sie das Dialogfeld **Eigenschaften** für dieses Richtlinienobjekt an und öffnen Sie die Registerkarte **Richtlinien**. Wählen Sie dann in der Liste die Richtlinie aus und klicken Sie auf **Anzeigen/Bearbeiten**, um das Dialogfeld **Eigenschaften der Gruppenobjekt-Deprovisionierungsrichtlinie** anzuzeigen. Klicken Sie auf die Registerkarte **Eigenschaften ändern**.

Die Registerkarte **Eigenschaften ändern** ähnelt der Seite mit demselben Namen in dem Assistenten, den Sie für die Erstellung des Richtlinienobjekts verwenden. Mit dieser Registerkarte können Sie wie folgt die Aktualisierungsregel für die Eigenschaft **Hinweise** hinzufügen:

1. Klicken Sie auf **Hinzufügen**, um das Dialogfeld **Objekteigenschaft wählen** anzuzeigen.
2. Aktivieren Sie das Kontrollkästchen neben der Eigenschaft **Hinweise** und klicken Sie dann auf **OK**.
3. Geben Sie im Dialogfeld **Wert hinzufügen Deprovisioned** in das Feld **'Hinweise' muss sein** ein und klicken Sie dann auf **OK**.

Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften der Gruppenobjekt-Deprovisionierungsrichtlinie** für das Richtlinienobjekt zu schließen.

Schritt 3: Anwenden des Richtlinienobjekts

Um das Richtlinienobjekt anzuwenden, können Sie im Dialogfeld **Eigenschaften** für dieses Richtlinienobjekt die Registerkarte **Bereich** verwenden:

1. Klicken Sie auf der Registerkarte **Bereich** auf die Schaltfläche **Bereich**, um das Fenster **Quest One ActiveRoles-Richtlinienbereich** für das zu verwaltende Richtlinienobjekt anzuzeigen.
2. Klicken Sie auf **Hinzufügen** und wählen Sie die Domäne, Organisationseinheit oder verwaltete Einheit aus, auf die Sie die Richtlinie anwenden möchten.
3. Klicken Sie auf **OK**, um das Fenster **Quest One ActiveRoles-Richtlinienbereich** zu schließen.
4. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** für das Richtlinienobjekt zu schließen.

Weitere Informationen bezüglich der Anwendung eines Richtlinienobjekts finden Sie unter Anwenden von Richtlinienobjekten und Verwalten des Richtlinienbereichs weiter oben in diesem Kapitel.

Gruppenobjekt-Verschiebung

Richtlinien dieser Kategorie dienen zum Automatisieren der Verschiebung von deprovisionierten Gruppenobjekten in angegebene Organisationseinheiten. So werden solche Gruppen der Steuerung der Administratoren entzogen, die die Organisationseinheiten verwalten, in denen sich diese Gruppen ursprünglich befanden. Eine Richtlinie dieser Kategorie kann auch so konfiguriert werden, dass sie deprovisionierte Gruppenobjekte nicht verschiebt.

Funktionsweise dieser Richtlinie

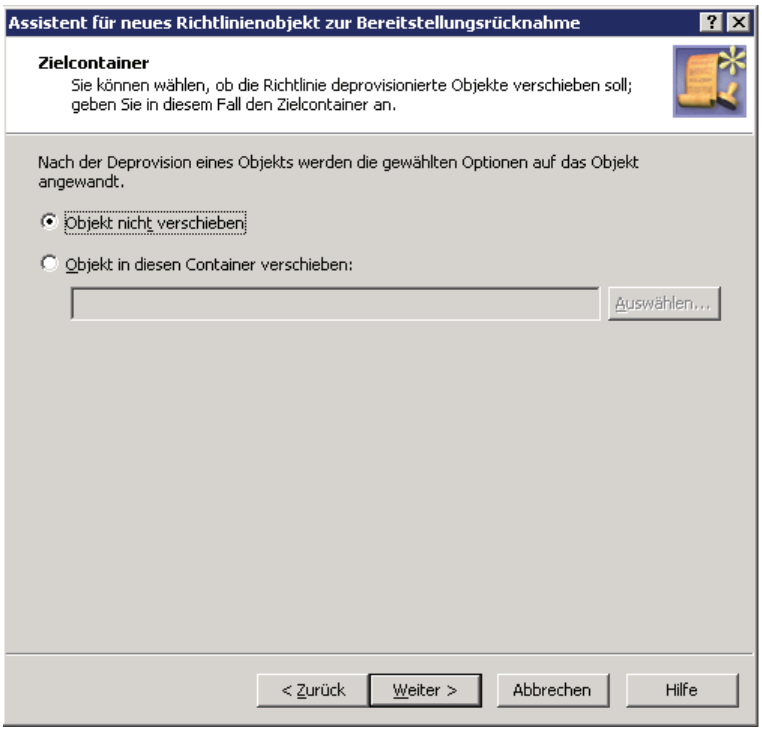
Beim Verarbeiten einer Deprovisionsanforderung für eine Gruppe verwendet Quest One ActiveRoles diese Richtlinie, um zu bestimmen, ob das deprovisionierte Gruppenobjekt in eine andere Organisationseinheit verschoben werden soll.

Eine für das Verschieben von Gruppenobjekten konfigurierte Richtlinie gibt auch das Ziel an, also die Organisationseinheit, in die Quest One ActiveRoles deprovisionierte Gruppenobjekte verschiebt.

Es kann auch eine Richtlinie konfiguriert werden, die Gruppenobjekte nicht verschiebt. Wenn eine solche Richtlinie auf einer bestimmten Ebene der Verzeichnishierarchie angewendet wird, setzt sie ggf. alle anderen Richtlinien dieser Kategorie außer Kraft, die auf einer höheren Ebene der Verzeichnishierarchie angewendet werden.

Konfigurieren einer Richtlinie zum Verschieben von Gruppenobjekten

Um eine Gruppenobjekt-Verschiebungsrichtlinie zu konfigurieren, wählen Sie **Gruppenobjekt-Verschiebung** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten „Neues Deprovisionsrichtlinienobjekt" oder im Assistenten „Deprovisionsrichtlinie hinzufügen" aus. Klicken Sie dann auf **Weiter**, damit die Seite **Zielcontainer** angezeigt wird.


Assistent für neues Richtlinienobjekt zur Bereitstellungsrücknahme
Zielcontainer
Sie können wählen, ob die Richtlinie deprovisionierte Objekte verschieben soll; geben Sie in diesem Fall den Zielcontainer an.
Nach der Deprovision eines Objekts werden die gewählten Optionen auf das Objekt angewandt.
Objekt nicht verschieben
Objekt in diesen Container verschieben:
Auswählen...
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite können Sie auswählen, ob die Richtlinie deprovisionierte Gruppenobjekte verschieben soll, und Sie können den Zielcontainer für den Verschiebungsvorgang auswählen.

Wählen Sie zunächst eine der folgenden Optionen aus:

- Klicken Sie auf **Objekt nicht verschieben**, damit die Richtlinie deprovisionierte Gruppenobjekte an ihren ursprünglichen Orten belässt. Mit dieser Option verbleibt jedes deprovisionierte Gruppenobjekt in der Organisationseinheit, in der es sich bei der Deprovisionierung befand.
- Klicken Sie auf **Objekt in diesen Container verschieben**, damit die Richtlinie deprovisionierte Gruppenobjekte in einen bestimmten Container verschiebt. Mit dieser Option wird jedes deprovisionierte Gruppenobjekt von seinem ursprünglichen Ort in eine angegebene Organisationseinheit verschoben.

Für die zweite Option müssen Sie die Organisationseinheit angeben, in die die Richtlinie deprovisionierte Gruppenobjekte verschieben soll. Klicken Sie auf die Schaltfläche **Auswählen** und wählen Sie dann die gewünschte Organisationseinheit aus.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Konfigurieren einer Richtlinie zum Verschieben von Gruppenobjekten

So konfigurieren Sie eine Richtlinie zum Verschieben von Gruppenobjekten:

1. Wählen Sie auf der Seite **Zu konfigurierende Richtlinie** die Option **Gruppenobjekt-Verschiebung** aus und klicken Sie dann auf **Weiter**.
2. Führen Sie auf der Seite **Zielcontainer** eine der folgenden Aktionen aus und klicken Sie dann auf **Weiter**:
   - Klicken Sie auf **Objekt nicht verschieben**, wenn die Richtlinie deprovisionierte Gruppenobjekte an ihren ursprünglichen Speicherorten belassen soll.
   - Klicken Sie auf **Objekt in diesen Container verschieben**, damit die Richtlinie die deprovisionierten Gruppenobjekte in einen bestimmten Container verschiebt. Klicken Sie dann auf **Wählen** und wählen Sie den gewünschten Container aus.
3. Auf der Seite **Richtlinie erzwingen** können Sie Objekte angeben, auf die dieses Richtlinienobjekt angewandt werden soll:
   - Klicken Sie auf **Hinzufügen** und verwenden Sie das Objekt **Objekte auswählen**, um die gewünschten Objekte auszuwählen.
4. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Szenario: Organisationseinheit zum Ablegen deprovisionierter Gruppen

In diesem Szenario wird das Konfigurieren einer Richtlinie beschrieben, die dazu führt, dass eine bestimmte Organisationseinheit alle deprovisionierten Gruppen enthält.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Nach der Deprovisionierung für eine Gruppe in dem Container, den Sie in Schritt 2 ausgewählt haben, verschiebt Quest One ActiveRoles folglich diese Gruppe automatisch in die von der Richtlinienkonfiguration bestimmte Organisationseinheit. In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten „Neues Deprovisionsrichtlinienobjekt" erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter Erstellen eines Richtlinienobjekts im Abschnitt Verwaltungsaufgaben für Richtlinienobjekte weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der **Richtlinie auf der Seite Richtlinientyp auswählen** des Assistenten auf **Gruppenobjekt-Verschiebung**. Klicken Sie dann auf **Weiter**.

Klicken Sie auf der Seite **Zielcontainer** auf **Objekt in diesen Container verschieben**. Klicken Sie dann auf die Schaltfläche **Auswählen**, um das Dialogfeld **Container suchen** anzuzeigen. Suchen Sie die Organisationseinheit, in die die Richtlinie deprovisionierte Gruppen verschieben soll, und wählen Sie sie aus. Klicken Sie dann auf **OK**.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten für neues Deprovisionsrichtlinienobjekt anwenden, oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen bezüglich der Anwendung eines Richtlinienobjekts finden Sie unter Anwenden von Richtlinienobjekten und Verwalten des Richtlinienbereichs weiter oben in diesem Kapitel.

Dauerhaftes Löschen des Gruppenobjekts

Richtlinien dieser Kategorie dienen zum Automatisieren der Löschung von deprovisionierten Gruppen. Deprovisionierte Gruppenobjekte werden für einen angegebenen Zeitraum beibehalten, bevor sie dauerhaft gelöscht werden. Eine Richtlinie dieser Kategorie kann auch so konfiguriert werden, dass sie deprovisionierte Gruppenobjekte nicht löscht.

Funktionsweise dieser Richtlinie

Beim Verarbeiten einer Deprovisionsanforderung für eine Gruppe verwendet Quest One ActiveRoles diese Richtlinie, um zu bestimmen, ob für das deprovisionierte Gruppenobjekt die Löschung geplant werden soll. Ein Gruppenobjekt, für das die Löschung geplant ist, wird nach einem bestimmten Zeitraum dauerhaft gelöscht. Dieser wird als *Wartezeitraum* bezeichnet.

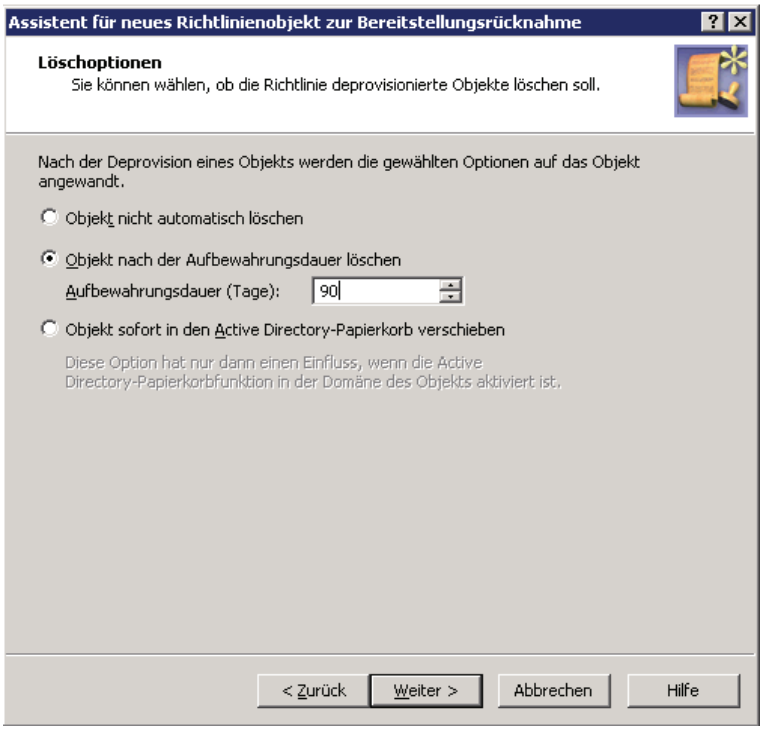
Eine Richtlinie, die zum Löschen von Gruppen konfiguriert ist, gibt an, für wie viele Tage deprovisionierte Gruppenobjekte beibehalten werden sollen. Mit einer solchen Richtlinie löscht Quest One ActiveRoles eine Gruppe nach der angegebenen Anzahl von Tagen seit der Deprovisionierung für die Gruppe dauerhaft.

Es kann auch eine Richtlinie konfiguriert werden, die Gruppen nicht löscht. Wenn eine solche Richtlinie auf einer bestimmten Ebene der Verzeichnishierarchie angewendet wird, setzt sie ggf. alle anderen Richtlinien dieser Kategorie außer Kraft, die auf einer höheren Ebene der Verzeichnishierarchie angewendet werden.

Eine weitere Option dieser Richtlinie gilt für Domänen, in denen die Active Directory-Papierkorbfunktion aktiviert ist. Die Richtlinie kann so konfiguriert werden, dass ein Gruppenobjekt direkt nach der Deprovisionierung der Gruppe in den Papierkorb verschoben wird (was bedeutet, dass die Gruppe sofort und ohne jeglichen Wartezeitraum gelöscht wird). Das Verschieben von deprovisionierten Gruppenobjekten in den Papierkorb kann aus Sicherheitsgründen als zusätzliche Maßnahme erforderlich sein. Der Active Directory-Papierkorb gewährleistet, dass das Gruppenobjekt bei Bedarf ohne jeglichen Datenverlust wiederhergestellt werden kann. Quest One ActiveRoles bietet die Möglichkeit, das Löschen von Gruppen, die in den Papierkorb deprovisioniert wurden, rückgängig zu machen und die Deprovisionierung dann aufzuheben.

Gehen Sie folgendermaßen vor, um einer Richtlinie zum permanenten Löschen eines Gruppenobjekts

Um eine Richtlinie bezüglich des permanenten Löschens eines Gruppenobjekts zu konfigurieren, wählen Sie **Permanentes Löschen eines Gruppenobjekts** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten „Neues Deprovisionsrichtlinienobjekt" oder im Assistenten „Deprovisionsrichtlinie hinzufügen" aus. Klicken Sie dann auf **Weiter**, damit die Seite **Löschoptionen** angezeigt wird.


Assistent für neues Richtlinienobjekt zur Bereitstellungsrücknahme
Löschoptionen
Sie können wählen, ob die Richtlinie deprovisionierte Objekte löschen soll.
Nach der Deprovision eines Objekts werden die gewählten Optionen auf das Objekt angewandt.
Objekt nicht automatisch löschen
Objekt nach der Aufbewahrungsdauer löschen
Aufbewahrungsdauer (Tage):
90
Objekt sofort in den Active Directory-Papierkorb verschieben
Diese Option hat nur dann einen Einfluss, wenn die Active Directory-Papierkorbfunktion in der Domäne des Objekts aktiviert ist.
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite können Sie auswählen, ob die Richtlinie für deprovisionierte Gruppen die Löschung planen soll. Außerdem können Sie angeben, für wie viele Tage deprovisionierte Gruppen beibehalten werden sollen.

Wählen Sie zunächst eine der folgenden Optionen aus:

- Klicken Sie auf **Objekt nicht automatisch löschen**, damit die Richtlinie deprovisionierte Gruppen nicht löscht.
- Klicken Sie auf **Objekt nach der Aufbewahrungsdauer löschen**, damit die Richtlinie für deprovisionierte Gruppen die Löschung plant.
- Klicken Sie auf **Objekt sofort in den Active Directory-Papierkorb verschieben**, damit die Richtlinie die deprovisionierten Gruppenobjekte in einen bestimmten Container verschiebt.

Wenn Sie die zweite Option auswählen, müssen Sie in dem Feld unter dieser Option eine Anzahl von Tagen angeben. Nachdem eine Gruppe deprovisioniert wurde und die angegebene Anzahl von Tagen vergangen ist, löscht Quest One ActiveRoles aufgrund der Richtlinie das Gruppenobjekt aus Active Directory.

Wenn Sie die dritte Option auswählen, sollten Sie diese Richtlinie auf Domänen anwenden, in denen der Active Directory-Papierkorb aktiviert ist; andernfalls hat die Richtlinie keine Auswirkungen. Bei Aktivierung dieser Option führt die Richtlinie, sobald eine Gruppe deprovisioniert wurde, dazu, dass Quest One ActiveRoles das Gruppenobjekt sofort löscht. In einer Domäne, in der der Active Directory-Papierkorb aktiviert ist, bedeutet dieser Löschvorgang bloß, dass das Objekt als gelöscht markiert und in einen bestimmten Container verschoben wird, aus dem es bei Bedarf ohne Datenverlust wiederhergestellt werden kann.

Konfigurieren einer Richtlinie zum dauerhaften Löschen von Gruppenobjekten

So konfigurieren Sie eine Richtlinie zum dauerhaften Löschen von Gruppenobjekten:

1. Wählen Sie auf der Seite **Zu konfigurierende Richtlinie** die Option **Permanentes Löschen eines Gruppenobjekts** aus und klicken Sie dann auf **Weiter**.
2. Führen Sie auf der Seite **Löschoptionen** eine der folgenden Aktionen aus und klicken Sie dann auf **Weiter**:
   - Klicken Sie auf **Objekt nicht automatisch löschen**, damit die Richtlinie deprovisionierte Gruppen nicht löscht.
   - Klicken Sie auf **Objekt nach der Aufbewahrungsdauer löschen**, damit die Richtlinie für deprovisionierte Gruppen die Löschung plant. Geben Sie dann unter **Aufbewahrungsdauer (Tage)** die Anzahl der Tage an, wie lange die deprovisionierte Gruppe beibehalten werden soll, bevor sie gelöscht wird.
   - Klicken Sie auf **Objekt sofort in den Active Directory-Papierkorb verschieben**, damit die Richtlinie die deprovisionierten Gruppenobjekte in einen bestimmten Container verschiebt.

   Wenn Sie die dritte Option auswählen, sollten Sie diese Richtlinie auf Domänen anwenden, in denen der Active Directory-Papierkorb aktiviert ist; andernfalls hat die Richtlinie keine Auswirkungen. Bei Aktivierung dieser Option führt die Richtlinie, sobald eine Gruppe deprovisioniert wurde, dazu, dass Quest One ActiveRoles das Gruppenobjekt sofort löscht. In einer Domäne, in der der Active Directory-Papierkorb aktiviert ist, bedeutet dieser Löschvorgang bloß, dass das Objekt als gelöscht markiert und in einen bestimmten Container verschoben wird, aus dem es bei Bedarf ohne Datenverlust wiederhergestellt werden kann.
3. Im Fenster **Richtlinie erzwingen** können Sie Objekte angeben, auf die dieses Richtlinienobjekt angewandt werden soll:
   - Klicken Sie auf **Hinzufügen** und verwenden Sie das Objekt **Objekte auswählen**, um die gewünschten Objekte auszuwählen.
4. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Szenario: Löschen von deprovisionierten Gruppen

In diesem Szenario wird beschrieben, wie Sie eine Richtlinie konfigurieren, damit Quest One ActiveRoles deprovisionierte Gruppen nach einem Wartezeitraum von 90 Tagen dauerhaft löscht.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert.
2. Wenden Sie das Richtlinienobjekt auf eine Domäne, Organisationseinheit oder verwaltete Einheit an.

Nach der Deprovisionierung einer Gruppe in dem Container, den Sie in Schritt 2 ausgewählt haben, behält Quest One ActiveRoles folglich das deprovisionierte Gruppenobjekt für 90 Tage bei und löscht das Objekt dann.

Schritt 1: Erstellen und Konfigurieren des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten „Neues Deprovisionsrichtlinienobjekt" erstellen und konfigurieren. Weitere Informationen über den Assistenten finden Sie unter Erstellen eines Richtlinienobjekts im Abschnitt Verwaltungsaufgaben für Richtlinienobjekte weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Richtlinientyp auswählen** des Assistenten auf **Permanentes Löschen eines Gruppenobjekts**. Klicken Sie dann auf **Weiter**.

Klicken Sie auf der Seite **Löschoptionen** auf **Objekt nach Wartezeitraum löschen**. Geben Sie dann in das Feld unter dieser Option den Wert **90** ein.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Schritt 2: Anwenden des Richtlinienobjekts

Sie können das Richtlinienobjekt mit Hilfe der Seite **Richtlinie erzwingen** im Assistenten für neues Deprovisionsrichtlinienobjekt anwenden, oder Sie können den Assistenten erst abschließen und dann den Befehl **Richtlinie erzwingen** für die Domäne, die Organisationseinheit oder die verwaltete Einheit verwenden, auf die Sie die Richtlinie anwenden möchten.

Weitere Informationen bezüglich der Anwendung eines Richtlinienobjekts finden Sie unter Anwenden von Richtlinienobjekten und Verwalten des Richtlinienbereichs weiter oben in diesem Kapitel.

Benachrichtigungsverteilung

Mit Richtlinien dieser Kategorie werden bei eingehenden Deprovisionierungsanforderungen automatisch E-Mail-Benachrichtigungen generiert und versendet. Der primäre Zweck einer solchen Richtlinie ist die Benachrichtigung ausgewählter Personen über die Deprovisionsanforderung für ein bestimmtes Objekt, damit sie notfalls entsprechende Aktionen ausführen können. Beim Konfigurieren einer Richtlinie dieser Kategorie können Sie eine Liste von Benachrichtigungsempfängern angeben. Außerdem können Sie Betreff und Text der Benachrichtigung anpassen.

Funktionsweise dieser Richtlinie

Beim Verarbeiten einer Deprovisionsanforderung verwendet Quest One ActiveRoles diese Richtlinie, um zu bestimmen, ob andere Personen über den angeforderten Deprovisionierungsvorgang informiert werden müssen. Dann generiert ActiveRoles Server ggf. eine Benachrichtigung und versendet sie an die Empfänger, die in der Richtlinienkonfiguration angegeben wurden.

Wenn ein Deprovisionierungsvorgang angefordert wird, gibt Quest One ActiveRoles unabhängig von den Vorgangsergebnissen eine Benachrichtigung aus. Daher stellt das Vorliegen einer Benachrichtigung keine Aussage über Erfolg oder Fehler des Vorgangs dar. Sie gibt statt dessen nur an, dass die Deprovisionierung angefordert wurde. Wenn Personen über die Ergebnisse der Deprovisionierung informiert werden sollen, sollten Sie die Richtlinie „Berichtsverteilung" verwenden, die im nächsten Abschnitt erörtert wird.

Die Benachrichtigungen werden pro Objekt ausgeführt: Jede Benachrichtigung enthält Informationen zu der Deprovisionsanforderung für ein einzelnes Objekt. Bei der Deprovisionierung mehrerer Objekte versendet Quest One ActiveRoles mehrere Benachrichtigungen, eine pro Objekt.

Quest One ActiveRoles sendet die Benachrichtigungen über einen SMTP-Server. Die Richtlinienkonfiguration gibt den SMTP-Server für ausgehende Nachrichten mit Hilfe von Quest One ActiveRoles-E-Mail-Einstellungen an, die den Namen des SMTP-Servers sowie für die Verbindungsherstellung notwendige Informationen enthalten.

Konfigurieren einer Benachrichtigungsübermittlungsrichtlinie

Um eine Benachrichtigungsübermittlungsrichtlinie zu konfigurieren, wählen Sie **Benachrichtigungsverteilung** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten „Neues Deprovisionsrichtlinienobjekt" oder im Assistenten „Deprovisionsrichtlinie hinzufügen" aus. Klicken Sie dann auf **Weiter**, damit die Seite **Empfänger und Nachricht der Benachrichtigung** angezeigt wird.

Auf der Seite **Empfänger und Nachricht der Benachrichtigung** können Sie eine Liste von Benachrichtigungsempfängern einrichten und ggf. alle notwendigen Änderungen am Betreff und Text der Nachricht vornehmen.

Klicken Sie zum Angeben von Benachrichtigungsempfängern auf die Schaltfläche neben dem Feld **Benachrichtigungsempfänger**, und geben Sie dann mindestens eine E-Mail-Adresse ein. Trennen Sie die Adressen der Benachrichtigungsempfänger mit Semikolons.

Wenn Sie die Benachrichtigungsmeldung ändern möchten, geben Sie Text in das Feld **Nachrichtenbetreff** oder **Nachrichtentext** ein. Sie können Makros verwenden, um Informationen zu dem zu deprovisionierenden Objekt einzugeben, damit die Nachricht für die Empfänger aussagekräftiger wird.

Makros haben dieselbe Syntax und Semantik wie Werte für Richtlinienbedingungen in Richtlinien zur Erzeugung und Validierung von Eigenschaften: Der LDAP-Anzeigename eines Attributs, eingeschlossen in spitze Klammern (<>) und mit einem Prozentzeichen (%) als Präfix, stellt den Wert dieses Attributs dar. Beispielsweise ersetzt Quest One ActiveRoles vor dem Senden einer Nachricht den Platzhalter %<name> durch den Namen des zu deprovisionierenden Objekts.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter**, um die Seite **Postausgangsserver** anzuzeigen.

Auf der Seite **Postausgangsserver** können Sie die in der Richtlinie zu verwendende E-Mail-Konfiguration auswählen. Außerdem können Sie E-Mail-Einstellungen in der ausgewählten Konfiguration anzeigen oder ändern.

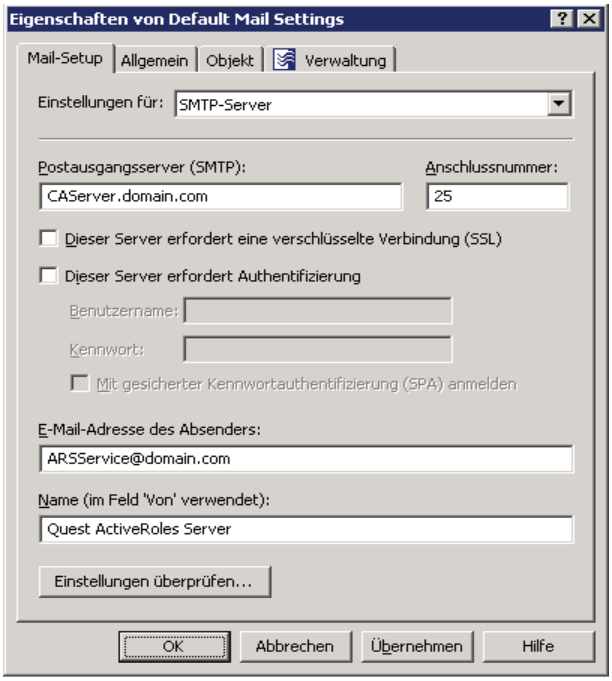
Wählen Sie zuerst in der Liste **Postausgangsserver (SMTP)** die E-Mail-Konfiguration aus, die von der Richtlinie verwendet werden soll.

Standardmäßig enthält die Liste **Postausgangsserver (SMTP)** einen einzelnen Eintrag. Mit der Quest One ActiveRoles-Konsole können Sie der Liste weitere Einträge hinzufügen. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration/Server Configuration**, klicken Sie mit der rechten Maustaste auf **Mail Configuration**, wählen Sie **Neu | Mail-Konfiguration** und folgen Sie dann den Anweisungen im Assistenten.

Jede E-Mail-Konfiguration gibt einen SMTP-Server an und stellt Informationen bereit, die zum Herstellen einer Verbindung mit diesem Server erforderlich sind. Um Konfigurationsparameter anzuzeigen und zu ändern, klicken Sie auf die Schaltfläche **Einstellungen**.

Konfigurieren von E-Mail-Einstellungen

Wenn Sie auf die **Schaltfläche** Einstellungen klicken, wird auf der Konsole das Dialogfeld **Eigenschaften** für die ausgewählte E-Mail-Konfiguration angezeigt. Dabei ähnelt die Registerkarte **Mail-Setup** der folgenden Abbildung.



Auf dieser Registerkarte können Sie die folgenden E-Mail-Einstellungen konfigurieren:

- **Postausgangsserver (SMTP).** Geben Sie die vollqualifizierte Adresse des zu verwendenden SMTP-Servers wie etwa smtp.mycompany.com ein.
- **Anschlussnummer.** Geben Sie die Portnummer auf dem SMTP-Server an, über die die Verbindung hergestellt werden soll. Normalerweise ist auf dem SMTP-Server diese Portnummer auf 25 festgelegt.
- **Dieser Server erfordert eine verschlüsselte Verbindung (SSL).** Aktivieren Sie dieses Kontrollkästchen, wenn der SMTP-Server erfordert, dass seine Clients Secure Sockets Layer (SSL) für das Veröffentlichen von Nachrichten über das Netzwerk verwenden.
- **Dieser Server erfordert Authentifizierung.** Aktivieren Sie dieses Kontrollkästchen, wenn der SMTP-Server für die Verwendung der Standard-Authentifizierung oder der Integrierten Windows-Authentifizierung konfiguriert ist. Geben Sie dann den Benutzernamen und das Kennwort in die Felder unter dieser Option ein. Quest One ActiveRoles übergibt diese Rechtezuweisungen bei der Verbindungseinrichtung an den SMTP-Server.
- **Mit gesicherter Kennwortauthentifizierung (SPA) anmelden.** Aktivieren Sie dieses Kontrollkästchen, wenn der SMTP-Server für die Verwendung der Integrierten Windows-Authentifizierung konfiguriert, um das eigentliche Benutzerkennwort nicht über das Netzwerk zu übertragen.

- **E-Mail-Adresse des Absenders.** Die Standard-E-Mail-Adresse des Nachrichtenabsenders. Es muss eine gültige E-Mail-Adresse angegeben werden. Normalerweise sollte dies die E-Mail-Adresse des vom Verwaltungsdienst verwendeten Dienstkontos sein.
- **Name (im Feld 'Von' verwendet).** Geben Sie den Standardnamen des Nachrichtenabsenders ein, der im Feld **Von** der mittels dieser E-Mail-Konfiguration gesendeten Nachrichten angezeigt werden soll.

Klicken Sie nach dem Konfigurieren der Einstellungen für den E-Mail-Server auf **OK**, um das Dialogfeld **Eigenschaften** für die E-Mail-Konfiguration zu schließen. Klicken Sie dann auf **Weiter** und befolgen Sie die Anweisungen im Assistenten, um das Richtlinienobjekt zu erstellen.

Verfahren zum Konfigurieren einer Benachrichtigungsübermittlungsrichtlinie

So konfigurieren Sie eine Richtlinie zur Benachrichtigungsübermittlung:

1. Wählen Sie auf der Seite **Zu konfigurierende Richtlinie** die Option **Richtlinie zur Benachrichtigungsübermittlung** aus und klicken Sie dann auf **Weiter**.
2. Gehen Sie auf der Seite **Empfänger und Nachricht der Benachrichtigung** wie nachfolgend beschrieben vor und klicken Sie dann auf **Weiter**:
   - Klicken Sie auf die Schaltfläche neben **Benachrichtigungsempfänger** und wählen Sie einen oder mehrere E-Mail-Empfänger aus.
   - Geben Sie unter **Nachrichtenbetreff** den Betreff der Nachricht ein, die die angegebenen Empfänger bei einer Anforderung zur Durchführung eines Deprovisionierungsvorgangs empfangen werden.
   - Geben Sie unter **Nachrichtentext** beliebige Informationen über den Deprovisionierungsvorgang ein.
3. Wählen Sie auf der Seite **Server für ausgehende Nachrichten** die E-Mail-Konfiguration aus, die von der Richtlinie verwendet werden soll. Klicken Sie in der Liste **Server für ausgehende E-Mails (SMTP)** auf die entsprechenden E-Mail-Einstellungen.
4. Wenn Sie die ausgewählten E-Mail-Einstellungen anzeigen oder ändern möchten, klicken Sie auf **Einstellungen** und verwenden Sie die Registerkarte **E-Mail-Einrichtung** (siehe Konfigurieren von E-Mail-Einstellungen weiter oben in diesem Kapitel).
5. Klicken Sie auf **Weiter**.
6. Auf der Seite **Richtlinie erzwingen** können Sie Objekte angeben, auf die dieses Richtlinienobjekt angewandt werden soll:
   - Klicken Sie auf **Hinzufügen** und verwenden Sie das Objekt **Objekte auswählen**, um die gewünschten Objekte auszuwählen.
7. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Szenario: Senden einer Deprovisionierungsbenachrichtigung an den Administrator

In diesem Szenario wird das Konfigurieren einer Richtlinie beschrieben, mit der der Administrator benachrichtigt wird, wenn Objekte in einer beliebigen bei Quest One ActiveRoles registrierten Domäne (verwalteten Domäne) deprovisioniert werden.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen Sie die entsprechende E-Mail-Konfiguration.
2. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert, und wenden Sie es an.

Folglich wird der Administrator bei einer Deprovisionsanforderung für ein Objekt wie etwa ein Benutzer oder eine Gruppe in einer beliebigen verwalteten Domäne mit Hilfe einer E-Mail-Nachricht über die Anforderung informiert. Die Nachricht umfasst den Namen des zu deprovisionierenden Objekts.

In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen der E-Mail-Konfiguration

In diesem Szenario wird Folgendes für Ihren SMTP-Server vorausgesetzt:

- Er wird auf dem Server **smtp.mycompany.com ausgeführt**
- Verwendet die **Standard-Portnummer (25)**
- Er lässt den **anonymen Zugriff zu**
- Er lässt **nicht verschlüsselte Verbindungen zu**

Außerdem wird vorausgesetzt, dass das Dienstkonto des Verwaltungsdienstes über ein Postfach mit der E-Mail-Adresse **ARSService@mycompany.com** verfügt.

Erstellen Sie die E-Mail-Konfiguration wie folgt mit Hilfe der Quest One ActiveRoles-Konsole:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Server Configuration**, klicken Sie mit der rechten Maustaste auf **Mail Configuration** und wählen Sie dann **Neu | Mail-Konfiguration**, um den Assistenten „Neue E-Mail-Konfiguration" zu starten.
2. Klicken Sie auf **Weiter**.
3. Geben Sie unter **Name** den Wert **Verbreitung der Deprovisionierungsbenachrichtigung** ein.
4. Klicken Sie auf **Weiter**.
5. Geben Sie unter **Postausgangsserver (SMTP)** den Wert **smtp.mycompany.com** ein.
6. Geben Sie im Feld **E-Mail-Adresse** des Absenders die E-Mail-Adresse des Dienstkontos ein. **ARSService@mycompany.com**.
7. Geben Sie im Feld **Name (im Feld 'Von' verwendet) Quest One ActiveRoles** ein.
8. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Schritt 2: Erstellen, Konfigurieren und Anwenden des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten „Neues Deprovisionsrichtlinienobjekt" erstellen, konfigurieren und anwenden. Weitere Informationen über den Assistenten finden Sie unter Erstellen eines Richtlinienobjekts im Abschnitt Verwaltungsaufgaben für Richtlinienobjekte weiter oben in diesem Kapitel.

Um die Richtlinie zu konfigurieren, klicken Sie auf **Benachrichtigungsverteilung** auf der Seite **Auswählen des Richtlinientyps** des Assistenten. Klicken Sie dann auf **Weiter**.

Klicken Sie auf der Seite **Empfänger und Nachricht der Benachrichtigung** auf die Schaltfläche neben dem Feld **Benachrichtigungsempfänger**, um das Dialogfeld **Empfänger der Benachrichtigung zur Deprovisionierung** anzuzeigen. Geben Sie in diesem Dialogfeld die E-Mail-Adresse des Administrators ein (z.B. administrator@mydomain.com) und klicken Sie dann auf **OK**.

Passen Sie dann den Betreff und den Text der Nachricht wie gewünscht an. Sie können beispielsweise den folgenden Betreff und Text eingeben:

Betreff der Nachricht

Deprovisionierung von %<Objektklasse> '%<Name>' angefordert

Text der Nachricht

Deprovisionierung von %<Objektklasse> '%<Name>' wird ausgeführt. Führen Sie bei Bedarf weitere Deprovisionsvorgänge durch, um die Deprovisionierung für diese %<Objektklasse> abzuschließen.

Diese Benachrichtigung wurde von Quest One ActiveRoles gemäß unternehmensweiten Richtlinien zur Deprovisionierung automatisch erzeugt.

Klicken Sie auf **Weiter** damit die Seite **Postausgangsserver** angezeigt wird.

Wählen Sie in der Liste im Feld **Postausgangsserver (SMTP)** die Option **Verbreitung der Deprovisionierungsbenachrichtigung** – die E-Mail-Konfiguration, die Sie in Schritt 1 erstellt haben. Klicken Sie dann auf **Weiter** damit die Seite **Richtlinie erzwingen** angezeigt wird.

Fügen Sie der Liste auf der Seite **Richtlinie erzwingen** den Ordner **Active Directory** wie folgt hinzu:

1. Klicken Sie auf die Schaltfläche **Hinzufügen**, um das Fenster **Objekte auswählen** anzuzeigen.
2. Klicken Sie im Fenster **Objekte auswählen** auf die Schaltfläche **Durchsuchen**, um das Dialogfeld **Container suchen** anzuzeigen.
3. Klicken Sie im Dialogfeld **Container suchen** auf **Active Directory** und klicken Sie dann auf **OK**.
4. Wählen Sie in der oberen Liste im Fenster **Objekte auswählen** den Eintrag **Active Directory** aus.
5. Klicken Sie auf **Hinzufügen** und dann auf **OK**, um das Fenster **Objekte auswählen** zu schließen.

Klicken Sie auf **Weiter** und klicken Sie dann auf **Fertig stellen**, um den Assistenten zu schließen.

Sie können auch in der Konsolenstruktur für den Ordner **Active Directory** den Befehl **Richtlinie erzwingen** verwenden, um die Richtlinie auf diesen Ordner anzuwenden. Weitere Informationen bezüglich der Anwendung eines Richtlinienobjekts finden Sie unter Anwenden von Richtlinienobjekten und Verwalten des Richtlinienbereichs weiter oben in diesem Kapitel.

Berichtsverteilung

Mit Richtlinien dieser Kategorie wird automatisch ein Bericht versendet, nachdem ein Deprovisionierungsvorgang abgeschlossen ist. Der Bericht enthält die Vorgangsergebnisse. Der primäre Zweck einer solchen Richtlinie ist es, bei Problemen während der Verarbeitung von Rücknahmeanforderungen ausgewählte Personen zu informieren. Diese Berichte werden weiter unten in diesem Kapitel beschrieben (siehe Abschnitt Bericht zu Ergebnissen der Deprovisionierung).

Die Berichte werden per E-Mail übermittelt. Beim Konfigurieren der Richtlinie zur Berichtübermittlung können Sie eine Liste von Berichtsempfängern einrichten, den Betreff der Berichtsnachrichten anpassen sowie angeben, ob bei Auftreten eines Fehlers ein Bericht gesendet werden soll oder nicht.

Funktionsweise dieser Richtlinie

Nach Abschluss eines Deprovisionierungsvorgangs ermittelt Quest One ActiveRoles anhand dieser Richtlinie, ob der Bericht mit den Ergebnissen der Deprovisionierung versendet werden muss. Dann generiert Quest One ActiveRoles die Berichtsnachricht und versendet sie an die Empfänger, die in der Richtlinienkonfiguration angegeben sind. Der Bericht schließt eine Liste der Aktionen ein, die während des Deprovisionierungsvorgangs ausgeführt wurden. Für jede Aktion gibt der Bericht an, ob sie erfolgreich abgeschlossen wurde, und stellt Informationen zu ihren Ergebnissen bereit.

Wenn die Richtlinie zur Berichtübermittlung so konfiguriert ist, dass keine Berichte gesendet werden, wenn keine Fehler aufgetreten sind, untersucht Quest One ActiveRoles die Deprovisionsergebnisse auf Fehler. Falls keine Fehler aufgetreten sind, wird der Bericht nicht versendet.

Quest One ActiveRoles generiert Berichte zur Deprovisionierung pro Objekt: Jede Berichtsnachricht enthält Informationen zur Deprovisionierung genau eines Objekts. Bei der Deprovisionierung mehrerer Objekte versendet Quest One ActiveRoles mehrere Berichtsnachrichten, eine pro deprovisioniertem Objekt.

Quest One ActiveRoles sendet die Berichtsnachrichten über einen SMTP-Server. Die Richtlinien-konfiguration gibt den SMTP-Server für ausgehende Nachrichten mit Hilfe von Quest One ActiveRoles-E-Mail-Einstellungen an, die den Namen des SMTP-Servers sowie für die Verbindungsherstellung notwendige Informationen enthalten.

Konfigurieren der Richtlinie „Berichtsverteilung"

Um die Richtlinie „Berichtsverteilung" zu konfigurieren, wählen Sie **Berichtsverteilung** auf der Seite **Zu konfigurierende Richtlinie** im Assistenten „Neues Deprovisionsrichtlinienobjekt" oder im Assistenten „Deprovisionsrichtlinie hinzufügen" aus. Klicken Sie dann auf **Weiter**, damit die Seite **Empfänger und Nachricht des Berichts** angezeigt wird.

Auf der Seite **Empfänger und Nachricht des Berichts** können Sie eine Liste von Berichtsempfängern einrichten, ggf. alle notwendigen Änderungen am Betreff der Nachricht ändern sowie angeben, ob die Richtlinie den Bericht auch dann versenden soll, wenn während des Deprovisionierungsvorgangs keine Fehler aufgetreten sind.

Klicken Sie zum Angeben von Berichtsempfängern auf die Schaltfläche neben dem Feld **Berichtsempfänger**, und geben Sie dann mindestens eine E-Mail-Adresse ein. Trennen Sie die Adressen der Benachrichtigungsempfänger mit Semikolons.

Wenn Sie den Betreff der Nachricht ändern möchten, geben Sie Text in das Feld **Nachrichtenbetreff** ein. Sie können Makros verwenden, um Informationen zu dem deprovisionierten Objekt einzugeben, damit die Nachricht für die Empfänger aussagekräftiger wird.

Makros haben dieselbe Syntax und Semantik wie Werte für Richtlinienbedingungen in Richtlinien zur Erzeugung und Validierung von Eigenschaften: Der LDAP-Anzeigename eines Attributs, eingeschlossen in spitze Klammern (<>) und mit einem Prozentzeichen (%) als Präfix, stellt den Wert dieses Attributs dar. Beispielsweise ersetzt Quest One ActiveRoles vor dem Senden einer Nachricht den Platzhalter %<name> durch den ursprünglichen Namen des deprovisionierten Objekts.

Quest One ActiveRoles ruft den Attributwert vor Beginn des Deprovisionierungsvorgangs ab, sodass der zu diesem Zeitpunkt aktuelle Wert vorliegt. Auch wenn eine Deprovisionsrichtlinie konfiguriert ist, die ein bestimmtes Attribut aktualisiert, wird für die Nachricht der ursprüngliche und nicht der aktualisierte Wert des Attributs gelesen.

Wenn die Richtlinie den Bericht unabhängig davon versenden soll, ob der Deprovisionierungsvorgang mit oder ohne Fehler abgeschlossen wurde, deaktivieren Sie das Kontrollkästchen **Bericht nur bei Fehlern aussenden**. Andernfalls wird der Bericht nicht gesendet, wenn das Objekt ohne Fehler deprovisioniert wurde.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter**, um die Seite **Postausgangsserver** anzuzeigen.

Diese Seite ähnelt der entsprechenden Assistentenseite zum Benachrichtigungsverteilung (siehe voriger Abschnitt). Sie können die in der Richtlinie zu verwendende E-Mail-Konfiguration auswählen. Außerdem können Sie E-Mail-Einstellungen in der ausgewählten Konfiguration anzeigen oder ändern.

Wählen Sie zuerst in der Liste **Postausgangsserver (SMTP)** die E-Mail-Konfiguration aus, die von der Richtlinie verwendet werden soll.

Standardmäßig enthält die Liste **Postausgangsserver (SMTP)** einen einzelnen Eintrag. Mit der Quest One ActiveRoles-Konsole können Sie der Liste weitere Einträge hinzufügen. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration/Server Configuration**, klicken Sie mit der rechten Maustaste auf **Mail Configuration**, wählen Sie **Neu | Mail-Konfiguration** und folgen Sie dann den Anweisungen im Assistenten.

Jede E-Mail-Konfiguration gibt einen SMTP-Server an und stellt Informationen bereit, die zum Herstellen einer Verbindung mit diesem Server erforderlich sind. Um Konfigurationsparameter anzuzeigen und zu ändern, klicken Sie auf die Schaltfläche **Einstellungen**. Anweisungen finden Sie im Abschnitt Konfigurieren von E-Mail-Einstellungen weiter oben in diesem Kapitel.

Klicken Sie nach Abschluss des Vorgangs auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um das Richtlinienobjekt zu erstellen.

Verfahren zum Konfigurieren einer Berichtübermittlungsrichtlinie

So konfigurieren Sie eine Richtlinie zur Berichtübermittlung:

1. Wählen Sie auf der Seite **Zu konfigurierende Richtlinie** die Option **Richtlinie zur Berichtübermittlung** aus und klicken Sie dann auf **Weiter**.
2. Gehen Sie auf der Seite **Empfänger und Nachricht des Berichts** wie nachfolgend beschrieben vor und klicken Sie dann auf **Weiter**:
   - Klicken Sie auf die Schaltfläche neben **Berichtsempfänger** und wählen Sie dann einen oder mehrere E-Mail-Empfänger aus.
   - Geben Sie unter **Nachrichtenbetreff** den Betreff der Nachricht ein, die die angegebenen Empfänger bei Abschluss eines Deprovisionierungsvorgangs empfangen werden.
   - Aktivieren Sie das Kontrollkästchen **Bericht nur bei Auftreten von Fehlern** senden, wenn die Richtlinie den Bericht nicht senden soll, wenn während des Deprovisionierungsvorgangs keine Fehler aufgetreten sind. Deaktivieren Sie das Kontrollkästchen, wenn die Richtlinie den Bericht unabhängig davon, ob Fehler aufgetreten sind oder nicht, senden soll.
3. Wählen Sie auf der Seite **Server für ausgehende Nachrichten** die E-Mail-Konfiguration aus, die von der Richtlinie verwendet werden soll. Klicken Sie in der Liste **Server für ausgehende E-Mails (SMTP)** auf die entsprechenden E-Mail-Einstellungen.
4. Wenn Sie die ausgewählten E-Mail-Einstellungen anzeigen oder ändern möchten, klicken Sie auf **Einstellungen** und verwenden Sie die Registerkarte **E-Mail-Einrichtung** (siehe Konfigurieren von E-Mail-Einstellungen weiter oben in diesem Kapitel).
5. Klicken Sie auf **Weiter**.

6. Auf der Seite **Richtlinie erzwingen** können Sie Objekte angeben, auf die dieses Richtlinienobjekt angewandt werden soll:
   - Klicken Sie auf **Hinzufügen** und verwenden Sie das Objekt **Objekte auswählen**, um die gewünschten Objekte auszuwählen.
7. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Szenario: Senden eines Deprovisionierungsberichts an den Administrator

In diesem Szenario wird beschrieben, wie Sie die folgende Richtlinie so konfigurieren, dass Deprovisionsvorgänge in allen bei Quest One ActiveRoles registrierten Domänen (verwalteten Domänen) überwacht werden:

- Überprüfen Sie nach Abschluss eines Deprovisionierungsvorgangs, ob während des Vorgangs Fehler aufgetreten sind.
- Wenn Fehler aufgetreten sind, wird der Bericht über die Deprovisionierungsergebnisse an den Administrator gesendet.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen Sie die entsprechende E-Mail-Konfiguration.
2. Erstellen und konfigurieren Sie das Richtlinienobjekt, das die entsprechende Richtlinie definiert, und wenden Sie es an.

Folglich erhält der Administrator nach Abschluss eines Deprovisionierungsvorgangs in einer beliebigen verwalteten Domäne einen Bericht, falls während des Vorgangs ein Fehler aufgetreten ist. Der Nachrichtenbetreff enthält den Namen des deprovisionierten Objekts.

In den folgenden beiden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen der E-Mail-Konfiguration

Sie können die im vorigen Abschnitt aufgeführten Anweisungen verwenden, um die E-Mail-Konfiguration zu erstellen (siehe Szenario: Senden einer Deprovisionierungsbenachrichtigung an den Administrator). Wenn Sie aufgefordert werden, einen Namen für die neuen Konfiguration einzugeben, geben Sie **Verbreitung des Deprovisionierungsberichts** ein.

Schritt 2: Erstellen, Konfigurieren und Anwenden des Richtlinienobjekts

Sie können das benötigte Richtlinienobjekt mit dem Assistenten „Neues Deprovisionsrichtlinienobjekt" erstellen, konfigurieren und anwenden. Weitere Informationen über den Assistenten finden Sie unter Erstellen eines Richtlinienobjekts im Abschnitt Verwaltungsaufgaben für Richtlinienobjekte weiter oben in diesem Kapitel.

Klicken Sie zum Konfigurieren der Richtlinie auf der Seite **Richtlinientyp auswählen** des Assistenten auf **Berichtsverteilung**. Klicken Sie dann auf **Weiter**.

Klicken Sie auf der Seite **Empfänger und Nachricht des Berichts** auf die Schaltfläche neben dem Feld **Berichtsempfänger**, um das Dialogfeld **Empfänger des Deprovisionierungsberichts** anzuzeigen. Geben Sie in diesem Dialogfeld die E-Mail-Adresse des Administrators ein (z.B. administrator@mydomain.com) und klicken Sie dann auf **OK**.

Passen Sie dann den Betreff der Nachricht wie gewünscht an. Sie können beispielsweise den folgenden Betreff eingeben: *Deprovisionierung von %<Objektklasse> '%<Name>' Abgeschlossen mit Fehlern*. Klicken Sie auf **Weiter** damit die Seite **Postausgangsserver** angezeigt wird.

Wählen Sie in der Liste im Feld **Postausgangsserver (SMTP)** den Eintrag **Verbreitung des Deprovisionierungsberichts** aus. Dabei handelt es sich um die E-Mail-Konfiguration, die Sie in Schritt 1 erstellt haben. Stellen Sie sicher, dass das Kontrollkästchen **Bericht nur bei Fehlern aussenden** aktiviert ist, und klicken Sie dann auf **Weiter**, um die Seite **Richtlinie erzwingen** anzuzeigen.

Klicken Sie auf der Seite **Richtlinie erzwingen** auf die Schaltfläche **Hinzufügen** und wählen Sie den Ordner **Active Directory** aus, um ihn der Liste hinzuzufügen. Eine detaillierte Anleitung finden Sie im vorigen Abschnitt (siehe Szenario: Senden einer Deprovisionierungsbenachrichtigung an den Administrator). Klicken Sie auf **Weiter** und klicken Sie dann auf **Fertig stellen**, um den Assistenten zu schließen.

Sie können auch in der Konsolenstruktur für den Ordner **Active Directory** den Befehl **Richtlinie erzwingen** verwenden, um die Richtlinie auf diesen Ordner anzuwenden. Weitere Informationen bezüglich der Anwendung eines Richtlinienobjekts finden Sie unter Anwenden von Richtlinienobjekten und Verwalten des Richtlinienbereichs weiter oben in diesem Kapitel.

Überlegungen bezüglich der Bereitstellung

Quest One ActiveRoles erzwingt die Umsetzung von Richtlinien, indem es Richtlinienobjekte anwendet, um die Datenintegrität im gesamten Verzeichnis zu fördern. Dies erfolgt durch die Generierung und Validierung der in das Verzeichnis eingegebenen Daten. Jedes Richtlinienobjekt ist im Wesentlichen ein Container, der einen oder mehrere Richtlinieneinträge (auch als Richtlinien bezeichnet) enthält. Es gibt verschiedene Arten von Richtlinieneinträgen, die innerhalb eines Richtlinienobjekts konfiguriert werden können. Die beiden wichtigsten Arten sind „Erzeugung und Validierung von Eigenschaften" und „Skriptausführung". Richtlinieneinträge des Typs „Erzeugung und Validierung von Eigenschaften" bieten eine so genannte Point-and-Click-Schnittstelle für die Erstellung grundlegender Regeln für das Füllen von Attributen. Richtlinieneinträge des Typs „Skriptausführung" ermöglichen die Nutzung des Scriptings für eine breite Palette von benutzerdefinierten Aktionen, die die standardmäßig in Quest One ActiveRoles enthaltenen Richtlinientypen ergänzen, erweitern oder ersetzen können.

Ebenso wie bei Gruppenrichtlinienobjekten in Active Directory ist der Speicherort, mit dem die Richtlinienobjekte von Quest One ActiveRoles verknüpft sind, entscheidend:

- Jegliche Richtlinien, die die gesamte Domäne beeinflussen, sollten sich in einem Richtlinienobjekt befinden, das auf Domänenebene verknüpft ist. Bei Bedarf können Filter genutzt werden, um bestimmte Objekte oder Containers (Organisationseinheiten) von der Verarbeitung durch diese Richtlinien auszuschließen.
- Wenn mehr als ein Objekt oder Container von den Auswirkungen einer domänenweiten Richtlinie ausgeschlossen werden sollen, empfiehlt es sich, diese Objekte oder Containers explizit in eine verwaltete Einheit aufzunehmen und dann mit Hilfe der Option **Vererbung blockieren** die Richtlinienfilterung auf diese verwaltete Einheit anzuwenden.

Ab dann ist es am besten, Richtlinien auf der obersten Ebene der Verzeichnisstruktur anzuwenden, die sie beeinflussen. Normalerweise sind Richtlinien jedoch nur erforderlich, um bestimmte Organisationseinheiten innerhalb der Gesamtstruktur zu beeinflussen. In diesem Fall ist eine verwaltete Einheit die effektivste Möglichkeit zur Anwendung der Richtlinien. Nehmen Sie die gewünschten Organisationseinheiten explizit in eine verwaltete Einheit auf und verknüpfen Sie das Richtlinienobjekt dann mit dieser verwalteten Einheit.

Eine Richtlinie besteht aus drei Hauptkomponenten. Diese sind nachfolgend aufgeführt:

- Ein Richtlinieneintrag, der die Richtlinie definiert.
- Ein Richtlinienobjekt, das diesen Richtlinieneintrag enthält.
- Eine Richtlinienobjektverknüpfung, die festlegt, wo die Richtlinie im Verzeichnis angewandt wird.

Normalerweise solle ein einzelnes Richtlinienobjekt alle Einträge für eine bestimmte Gruppe von Richtlinien umfassen. Es ist nicht effizient, einen Eintrag je Richtlinienobjekt zu erstellen, da dies nicht dem Sinn und Zweck der Trennung zwischen Richtlinienobjekt und Richtlinieneinträgen entspricht.

Eine Richtlinie kann nicht für eine bestimmte Administratorengruppe gefiltert werden. Nach Anwendung auf ein bestimmtes Objekt oder einen bestimmten Container gilt eine Richtlinie unter allen Bedingungen für jeden Administrator. Dies gilt, sofern nicht eine Skriptausführungsrichtlinie als ein Richtlinieneintrag enthalten ist, die die Schnittstelle **IEDSEffectivePolicyRequest** nutzt, um die von anderen Richtlinieneinträgen festgelegten Richtlinien zu umgehen. Diese Schnittstelle ist im Quest One ActiveRoles SDK dokumentiert.

Skriptausführungsrichtlinien sind Richtlinieneinträge, die in einer Scripting-Sprache wie etwa Microsoft Windows PowerShell oder VBScript geschriebene Skripte nutzen. Richtlinienskripte nutzen Ereignishandler, die vor oder nach jeder Aktion, die sich in einem Verzeichnis ereignen können, ausgeführt werden. Die folgende Tabelle enthält eine Liste dieser Handler:

NAME	BESCHREIBUNG
onPreCreate	Übernimmt bei einer auf einen Container angewandten Skriptrichtlinie bei Erhalt einer Anforderung zur Erstellung eines Objekts in diesem Container die Kontrolle. Aktiviert ein Skript zur Ausführung benutzerdefinierter Vorgänge vor der Erstellung eines Objekts.
onPostCreate	Übernimmt bei einer auf einen Container angewandten Skriptrichtlinie nach Abschluss einer Anforderung zur Erstellung eines Objekts in diesem Container die Kontrolle. Aktiviert ein Skript zur Ausführung benutzerdefinierter Vorgänge nach der Erstellung eines Objekts.
onPreDelete	Übernimmt bei Erhalt einer Anforderung zum Löschen eines Objekts die Kontrolle. Aktiviert ein Skript zur Ausführung von benutzerdefinierten Vorgängen vor dem Löschen eines Objekts.
onPostDelete	Übernimmt nach Abschluss einer Anforderung zum Löschen eines Objekts die Kontrolle. Aktiviert ein Skript zur Ausführung von benutzerdefinierten Vorgängen nach dem Löschen eines Objekts.
onPreModify	Übernimmt bei Erhalt einer Anforderung zum Starten der Änderung der Objekteigenschaften die Kontrolle. Aktiviert ein Skript zur Ausführung von benutzerdefinierten Vorgängen vor der Anwendung von Änderungen auf ein Objekt.
onPostModify	Übernimmt nach Abschluss einer Anforderung zum Ändern von Objekteigenschaften die Kontrolle. Aktiviert ein Skript zur Ausführung von benutzerdefinierten Vorgängen nach der Änderung der Eigenschaftswerte eines Objekts.
onPreMove	Übernimmt bei einer auf einen Container angewandten Skriptrichtlinie bei Erhalt einer Anforderung zum Starten der Verschiebung eines Objekts aus diesem Container die Kontrolle. Aktiviert ein Skript zur Ausführung benutzerdefinierter Vorgänge vor dem Verschieben eines Objekts.
onPostMove	Übernimmt bei einer auf einen Container angewandten Skriptrichtlinie nach Abschluss einer Anforderung zum Verschieben eines Objekts in diesen Container die Kontrolle. Aktiviert ein Skript zur Ausführung benutzerdefinierter Vorgänge nach dem Verschieben eines Objekts.
onPreRename	Übernimmt bei Erhalt einer Anforderung zum Starten der Umbenennung eines Objekts die Kontrolle. Aktiviert ein Skript zur Ausführung von benutzerdefinierten Vorgängen vor dem Umbenennen eines Objekts.
onPostRename	Übernimmt nach Abschluss einer Anforderung zum Umbenennen eines Objekts die Kontrolle. Aktiviert ein Skript zur Ausführung von benutzerdefinierten Vorgängen nach dem Umbenennen eines Objekts.
onPreGet	Übernimmt bei Erhalt einer Anforderung zum Abrufen von Objekteigenschaften die Kontrolle. Aktiviert ein Skript zur Ausführung von benutzerdefinierten Vorgängen vor dem Start des Abrufens der Eigenschaftswerte eines Objekts.
onPostGet	Übernimmt nach Abschluss einer Anforderung zum Abrufen von Objekteigenschaften die Kontrolle. Aktiviert ein Skript zur Ausführung von benutzerdefinierten Vorgängen nach dem Abrufen der Eigenschaftswerte eines Objekts.
onPreSearch	Übernimmt bei Erhalt einer Anforderung zum Starten einer Suche die Kontrolle. Aktiviert ein Skript zur Ausführung von benutzerdefinierten Vorgängen vor dem Starten einer Suche.
onPreDeprovision	Übernimmt bei Erhalt einer Anforderung zur Ausführung des Deprovisionierungsvorgangs die Kontrolle. Aktiviert ein Skript zur Ausführung von benutzerdefinierten Vorgängen vor dem Start des Vorgangs.

NAME	BESCHREIBUNG
onDeprovision	Übernimmt im Verlauf der Verarbeitung einer Anforderung zur Ausführung des Deprovisionierungsvorgangs die Kontrolle. Ermöglicht die Verwendung eines Skripts zur Anpassung des Verhaltens des Vorgangs.
onPostDeprovision	Übernimmt nach Abschluss einer Anforderung zur Ausführung des Deprovisionierungsvorgangs die Kontrolle. Aktiviert ein Skript zur Ausführung benutzerdefinierter Vorgänge nach dem Vorgang.
onPreUnDeprovision	Übernimmt bei Erhalt einer Anforderung zur Ausführung der Aufhebung des Deprovisionierungsvorgangs die Kontrolle. Aktiviert ein Skript zur Ausführung von benutzerdefinierten Vorgängen vor dem Start des Vorgangs.
onUnDeprovision	Übernimmt im Verlauf der Verarbeitung einer Anforderung zur Ausführung der Aufhebung des Deprovisionierungsvorgangs die Kontrolle. Ermöglicht die Verwendung eines Skripts zur Anpassung des Verhaltens des Vorgangs.
onPostUnDeprovision	Übernimmt nach Abschluss einer Anforderung zur Ausführung der Aufhebung des Deprovisionierungsvorgangs die Kontrolle. Aktiviert ein Skript zur Ausführung benutzerdefinierter Vorgänge nach dem Vorgang.
onPreUnDelete	Übernimmt bei Erhalt einer Anforderung zur Ausführung des Wiederherstellungsvorgangs die Kontrolle. Aktiviert ein Skript zur Ausführung von benutzerdefinierten Vorgängen vor dem Start des Vorgangs.
onPostUnDelete	Übernimmt nach Abschluss einer Anforderung zur Ausführung des Wiederherstellungsvorgangs die Kontrolle. Aktiviert ein Skript zur Ausführung benutzerdefinierter Vorgänge nach dem Vorgang.
onCheckPropertyValues	Übernimmt bei Erhalt einer Anforderung zur Überprüfung und Bestätigung der Änderungen, die an einem Objekt vorgenommen werden sollen, die Kontrolle. Aktiviert ein Skript zur Ausführung benutzerdefinierter Vorgänge nach normalen Gültigkeitsprüfungen an einem Objekt.
onGetEffectivePolicy	Übernimmt bei Erhalt einer Anforderung zum Abrufen der Richtlinieneinstellungen, die für ein bestimmtes Objekt gelten (wie etwa hinsichtlich der Eigenschaftswerte geltende Richtlinieneinschränkungen), die Kontrolle. Aktiviert ein Skript zur Ausführung benutzerdefinierter Vorgänge nach dem Abrufen von Richtlinieneinstellungen.
onInit	Übernimmt die Kontrolle, wenn der Verwaltungsdienst die Definition der Skriptparameter abfragt, und ermöglicht dem Skript, den Namen und andere Merkmale jedes Parameters zu offenbaren.
onFilter	Funktion mit booleschem Wert, der während der Ausführung des Ereignishandlers onPreSearch ausgewertet wird und es ermöglicht, Suchergebnisse auf Basis der Eigenschaften der bei der Suche gefundenen Objekte zu filtern. Ausführlichere Informationen finden Sie unter „IEDSRequestParameters Properties" imQuest One ActiveRoles SDK.

Wenn eine Aktion ausgeführt wird, überprüft Quest One ActiveRoles, ob jegliche Richtlinienobjekte angewandt wurden, die über Skriptausführungsrichtlinien verfügen. Ist dies der Fall, wird das Richtlinienskript dahingehend überprüft, ob es einen Ereignishandler für die jeweilige ausgeführte Aktion enthält. Das Objekt, auf das die Aktion angewandt wird, wird für weitere Aktionen an den Ereignishandler weitergeleitet. Diese Ereignishandler werden in der Regel im Sicherheitskontext des Dienstkontos ausgeführt, selbst wenn ein Benutzer also nicht die erforderlichen Rechte besitzen sollte, um die im Richtlinienskript angegebenen Aktionen auszuführen, wird dieses dennoch korrekt ausgeführt. Sollten während der Ausführung eines Richtlinienskripts Fehler auftreten, können diese Fehler bei Post-Aktionshandlern im „EDM Server"-Ereignisprotokoll gefunden werden und werden bei Prä-Aktionshandlern dem Client angezeigt.

Richtlinienskripts werden in der Regel in einer Skriptsprache wie Windows PowerShell oder VBScript verfasst. Viele Beispielskripts basierend auf Windows PowerShell und VBScript sowie Anweisungen zur Verwendung des Quest One ActiveRoles ADSI-Provider sowohl für Richtlinien- als auch für eigenständige Skripts finden Sie im Quest One ActiveRoles SDK.

Ebenfalls muss angemerkt werden, dass Richtlinienskripts ebenfalls bei nativen Verzeichnisänderungen ausgelöst und ausgeführt werden können. Zur Aktivierung dieses Verhaltens sollten Sie die Option wählen, welche das Richtlinienskript zur Handhabung von durch die Verzeichnissynchronisation gemeldeten Verzeichnisänderungen anleitet (wählen Sie das Kontrollkästchen **Änderungen von DirSync-Steuerung handhaben** auf der Registerkarte **Skriptmodul** im Dialogfeld **Eigenschaften** für den jeweiligen Richtlinieneintrag) und die Schnittstelle **IEDSRequestParameters** in einem Post-Aktions-Ereignishandler verwenden. Weitere Informationen zu diesem Thema finden Sie in der Quest One ActiveRoles SDK-Dokumentation.

Zum Verfassen von eigenständigen Skripts, welche den Quest One ActiveRoles ADSI-Provider verwenden, müssen Sie das Quest One ActiveRoles SDK installieren. Das Quest One ActiveRoles SDK wird normalerweise als Teil der Verwaltungsdienst-Installation von Quest One ActiveRoles installiert, kann aber auch separat installiert werden (beziehen Sie sich für weitere Informationen auf die *Quest One ActiveRoles-Schnellstartanleitung*). Bei einer separaten Installation erstellt das Quest One ActiveRoles SDK eine lokale, eigenständige Installation des Quest One ActiveRoles ADSI-Provider. Ebenfalls stellt es eine Hilfedatei bereit, die eine Dokumentation für Skriptautoren enthält. Alle Skripts, welche den Quest One ActiveRoles ADSI-Provider zum Zugriff auf das Verzeichnis verwenden, unterliegen sämtlichen innerhalb der Quest One ActiveRoles-Umgebung geltenden Delegationen und Richtlinien, was die Integrität Ihrer Verzeichnisdaten gewährleistet.

Überprüfen der Richtlinieneinhaltung

Beim Überprüfen auf Richtlinieneinhaltung werden Informationen zu Verzeichnisdaten bereitgestellt, die den mit Quest One ActiveRoles definierten Richtlinien nicht entsprechen, z.B. Namenskonventionen für Benutzer oder Gruppen. Wenn Sie Richtlinien definieren, nachdem bereits Daten eingegeben wurden, können Sie die Daten überprüfen und sie entsprechend ändern, um sicherzustellen, dass sie die Richtlinienanforderungen erfüllen.

Zwar können mit Quest One ActiveRoles Geschäftsregeln und Richtlinien normalerweise nicht mehr umgangen werden, nachdem sie konfiguriert sind; es gibt jedoch Situationen, in denen die tatsächlichen Verzeichnisdaten möglicherweise einige der vorgeschriebenen Richtlinien oder Geschäftsregeln verletzen. Beispielsweise überprüft Quest One ActiveRoles beim Anwenden einer neuen Richtlinie nicht automatisch die vorhandenen Verzeichnisdaten, um zu ermitteln, ob sie der neuen Richtlinie entsprechen. Ein weiteres Beispiel ist ein Prozess, der automatisch neue Objekte wie etwa Benutzer- oder Gruppenobjekte erstellt, indem er direkt auf Active Directory zugreift und Quest One ActiveRoles nicht verwendet.

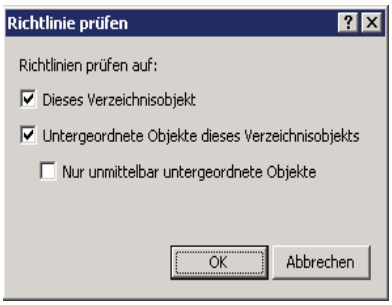
Das Berichterstattungspaket von Quest One ActiveRoles enthält eine Reihe von Berichten, die bei der Erkennung von Richtlinienübertretungen in Verzeichnisdaten helfen, indem sie Informationen zum Zustand der Verzeichnisobjekte im Verhältnis zu den vorgeschriebenen Richtlinien sammeln und analysieren. Da das Abrufen derartiger Informationen jedoch zeitintensiv und aufwändig sein kann, ermöglichen die Berichte zur Richtlinieneinhaltung es manchmal nicht, richtlinienbezogene Probleme zeitnah zu lösen.

Um diesem Problem zu begegnen, ermöglicht Quest One ActiveRoles die schnelle Erstellung und Untersuchung von Richtlinienüberprüfungsergebnissen für einzelne Objekte oder gesamte Container. Die Richtlinienüberprüfungsergebnisse stellen eine Liste von Verzeichnisobjekten bereit, die Richtlinien verletzen, und beschreiben die erkannten Verletzungen. Anhand der Richtlinienüberprüfungsergebnisse können Sie geeignete Änderungen an Objekten oder Richtlinien vornehmen:

- Ändern von Objekteigenschaften in Übereinstimmung mit Richtlinien.
- Verhindern der Auswirkung bestimmter Richtlinien auf einzelne Objekte.
- Ändern von Richtlinienobjekten nach Bedarf.
- Ausführen einer Verwaltungsaufgabe, z.B. Deaktivieren oder Verschieben von Benutzerobjekten, die Regeln verletzen.

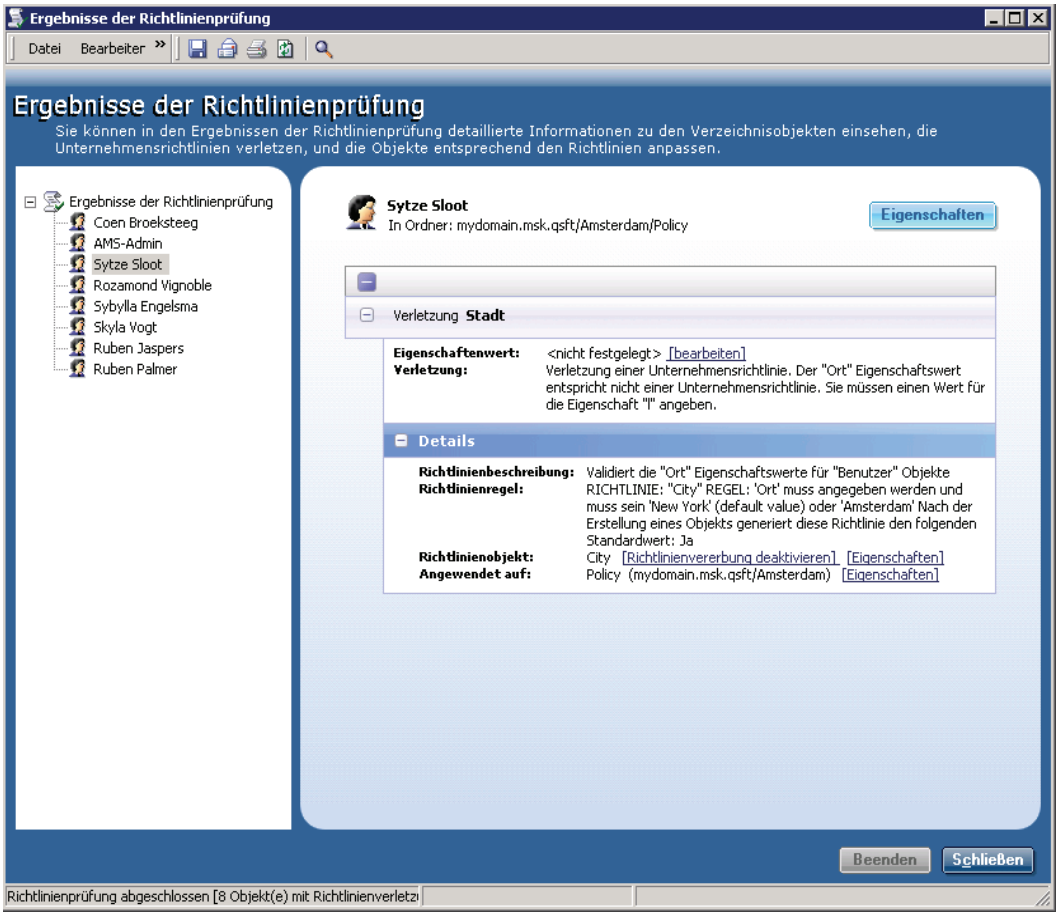
Zusätzlich können Sie Richtlinienüberprüfungsergebnisse in einer Datei speichern, drucken oder an einen E-Mail-Empfänger senden.

Um die Richtlinieneinhaltung eines Objekts zu überprüfen, klicken Sie mit der rechten Maustaste auf das Objekt und klicken dann auf **Richtlinie prüfen**. Bei einem Containerobjekt wird nun das Dialogfeld **Richtlinie prüfen** angezeigt, das in der folgenden Abbildung gezeigt wird.



Aktivieren Sie im Dialogfeld **Richtlinie prüfen** die entsprechenden Kontrollkästchen, um den Bereich des Vorgangs anzugeben, und klicken dann auf **OK**.

Das Fenster **Ergebnisse der Richtlinienprüfung** wird angezeigt, und der Vorgang wird gestartet. Die Überprüfungsergebnisse werden im rechten Bereich des Fensters angezeigt (siehe Abbildung unten).


Ergebnisse der Richtlinienprüfung
Datei
Bearbeiter
Ergebnisse der Richtlinienprüfung
Sie können in den Ergebnissen der Richtlinienprüfung detaillierte Informationen zu den Verzeichnisobjekten einsehen, die Unternehmensrichtlinien verletzen, und die Objekte entsprechend den Richtlinien anpassen.
Ergebnisse der Richtlinienprüfung
Coen Broeksteeg
AMS-Admin
Sytze Sloot
Rozamond Vignoble
Sybylla Engelsma
Skyla Vogt
Ruben Jaspers
Ruben Palmer
Sytze Sloot
In Ordner: mydomain.msk.qsft/Amsterdam/Policy
Eigenschaften
Verletzung Stadt
Eigenschaftenwert: <nicht festgelegt> [bearbeiten]
Verletzung: Verletzung einer Unternehmensrichtlinie. Der "Ort" Eigenschaftswert entspricht nicht einer Unternehmensrichtlinie. Sie müssen einen Wert für die Eigenschaft "l" angeben.
Details
Richtlinienbeschreibung: Validiert die "Ort" Eigenschaftswerte für "Benutzer" Objekte
Richtlinienregel: RICHTLINIE: "City" REGEL: 'Ort' muss angegeben werden und muss sein 'New York' (default value) oder 'Amsterdam' Nach der Erstellung eines Objekts generiert diese Richtlinie den folgenden Standardwert: Ja
Richtlinienobjekt: City [Richtlinienvererbung deaktivieren] [Eigenschaften]
Angewendet auf: Policy (mydomain.msk.qsft/Amsterdam) [Eigenschaften]
Beenden
Schließen
Richtlinienprüfung abgeschlossen [8 Objekt(e) mit Richtlinienverletzu

Die Objekte, die eine Richtlinie verletzen, werden im linken Bereich angezeigt. Wenn Sie im linken Bereich auf ein Objekt klicken, wird die Richtlinienverletzung im rechten Bereich detailliert beschrieben.

Standardmäßig werden im rechten Bereich des Fensters **Ergebnisse der Richtlinienprüfung** nur grundlegende Optionen angezeigt. Sie können mehrere Optionen anzeigen, indem Sie auf die Spaltenüberschrift der Spalte **Details** klicken.

Mit Hilfe der Verknüpfungen im linken Bereich können Sie folgende Aufgaben ausführen:

- Ändern des Eigenschaftswerts, der die Richtlinie verletzt: Klicken Sie auf die Verknüpfung **bearbeiten** neben der Bezeichnung **Eigenschaftenwert**.
- Entfernen des Objekts aus dem Bereich der Richtlinie: Klicken Sie auf die Verknüpfung **Richtlinienvererbung deaktivieren** neben der Bezeichnung **Richtlinienobjekt**. Dann steuert die Richtlinie das Objekt nicht mehr.
- Ändern der Richtlinie: Klicken Sie auf die Verknüpfung **Eigenschaften** neben der Bezeichnung **Richtlinienobjekt**. Dies zeigt das Dialogfeld **Eigenschaften** für das Richtlinienobjekt an, das unter „Hinzufügen, Ändern und Entfernen von Richtlinien" weiter oben in diesem Kapitel beschrieben ist.

- Verwalten des Objekts, das die Richtlinie verletzt: Klicken Sie oben rechts im rechten Bereich auf die Schaltfläche **Eigenschaften**
- Verwalten des Objekts, auf das das Richtlinienobjekt angewendet wird: Klicken Sie auf die Verknüpfung **Eigenschaften** neben der Bezeichnung **Angewendet auf**.

Sie können sich anhand der folgenden Anweisungen mit dem Überprüfen der Richtlinieneinhaltung über die Quest One ActiveRoles-Konsole vertraut machen:

1. Erstellen und konfigurieren Sie ein Richtlinienobjekt mit der Richtlinie für die Generierung und Validierung von Eigenschaften für die Eigenschaft **Abteilung** von Benutzerobjekten. Geben Sie dabei die Richtlinienregel wie folgt an: *Wert muss angegeben werden und muss „Sales" oder „Production" lauten*.
2. Wenden Sie dieses Richtlinienobjekt auf eine Organisationseinheit an, die bereits Benutzerobjekte ohne Angabe der Abteilung enthält (verknüpfen Sie es mit ihr).
3. Klicken Sie mit der rechten Maustaste auf die Organisationseinheit und klicken Sie dann auf **Richtlinie prüfen**. Klicken Sie im Dialogfeld **Richtlinie prüfen** auf **OK**

   *Nachdem Sie diese Schritte ausgeführt haben, wird das Fenster **Ergebnisse der Richtlinienprüfung** angezeigt. In seinem linken Bereich sind Objekte aufgelistet, die die Richtlinie verletzen.*
4. Warten Sie, während die Liste im linken Bereich aufgefüllt wird. Wählen Sie dann in der Liste ein Benutzerobjekt aus.

   *Im rechten Bereich neben der Bezeichnung **Verletzung** wird die Eingabeaufforderung „Sie müssen einen Wert für die Eigenschaft 'Abteilung' angeben" angezeigt.*
5. Klicken Sie im rechten Bereich auf die Verknüpfung **Bearbeiten** neben der Bezeichnung **Eigenschaftenwert**.
6. Wählen Sie im Dialogfeld **Eigenschaften** im Kombinationsfeld **Abteilung** einen der zulässigen Werte (**Production** oder **Sales**) aus.

Verfahren zur Überprüfung der Richtlinieneinhaltung

Beim Überprüfen auf Richtlinieneinhaltung werden Informationen zu Verzeichnisdaten bereitgestellt, die den mit Quest One ActiveRoles definierten Richtlinien nicht entsprechen, z.B. Namenskonventionen für Benutzer oder Gruppen. Wenn Sie Richtlinien definieren, nachdem bereits Daten eingegeben wurden, können Sie die Daten überprüfen und sie entsprechend ändern, um sicherzustellen, dass sie die Richtlinienanforderungen erfüllen.

Gehen Sie folgendermaßen vor, um ein Objekt auf seine Richtlinienkonformität hin zu überprüfen:

1. Klicken Sie mit der rechten Maustaste auf das Objekt und klicken Sie dann auf **Richtlinie prüfen**.
2. Wenn das Objekt ein Container oder eine verwaltete Einheit ist, aktivieren Sie eine entsprechende Kombination dieser Kontrollkästchen, um den Bereich des Vorgangs festzulegen, und klicken Sie dann auf **OK**:
   - **Dieses Verzeichnisobjekt.** Der Bereich umfasst den Container oder die verwaltete Einheit, den bzw. die Sie ausgewählt haben (diese Option führt nicht dazu, dass der Bereich die untergeordneten Objekte oder Mitglieder des Containers oder der verwalteten Einheit enthält).
   - **Untergeordnete Objekte dieses Verzeichnisobjekts.** Der Bereich umfasst alle untergeordneten Objekte (oder Mitglieder bei Anwendung auf eine verwaltete Einheit) in der gesamten Hierarchie unter dem von Ihnen ausgewählten Container oder unter der von Ihnen ausgewählten verwalteten Einheit.

- **Nur unmittelbar untergeordnete Objekte.** Der Bereich umfasst nur die untergeordneten Objekte (oder Mitglieder bei einer verwalteten Einheit), denen der von Ihnen ausgewählte Container oder die von Ihnen ausgewählte verwaltete Einheit direkt übergeordnet ist.

*Der Fortschritt und die Ergebnisse des Richtlinienüberprüfungsvorgangs werden im Fenster **Ergebnisse der Richtlinienprüfung** angezeigt. Im linken Bereich des Fensters sind die Objekte aufgelistet, für die ein Richtlinienverstoß erkannt wurde.*

3. Klicken Sie auf ein Objekt im linken Bereich des Fensters **Ergebnisse der Richtlinienprüfung**.

   *Wenn Sie im linken Bereich auf ein Objekt klicken, wird die Richtlinienverletzung im rechten Bereich detailliert beschrieben. Standardmäßig werden im rechten Bereich des Fensters **Ergebnisse der Richtlinienprüfung** nur grundlegende Optionen angezeigt. Sie können mehrere Optionen anzeigen, indem Sie auf die Spaltenüberschrift der Spalte **Details** klicken.*

4. Verwenden Sie Hypertext-Verknüpfungen im rechten Bereich, um die folgenden Aufgaben auszuführen:
   - Ändern des Eigenschaftswerts, der die Richtlinie verletzt: Klicken Sie auf die Verknüpfung **bearbeiten** neben der Bezeichnung **Eigenschaftenwert**.
   - Entfernen des Objekts aus dem Bereich der Richtlinie: Klicken Sie auf die Verknüpfung **Richtlinienvererbung deaktivieren** neben der Bezeichnung **Richtlinienobjekt**. Dann steuert die Richtlinie das Objekt nicht mehr.
   - Ändern der Richtlinie: Klicken Sie auf die Verknüpfung **Eigenschaften** neben der Bezeichnung **Richtlinienobjekt**. Hierdurch wird das Dialogfeld **Eigenschaften** für das Richtlinienobjekt angezeigt. Anweisungen bezüglich des Hinzufügens, Änderns oder Entfernens von Richtlinien zum bzw. aus dem Dialogfeld **Eigenschaften** finden Sie unter Hinzufügen, Ändern und Entfernen von Richtlinien weiter oben in diesem Dokument.
   - Zeigen Sie die Eigenschaften des Objekts an, das gegen die Richtlinie verstößt, und ändern Sie sie: Klicken Sie oben rechts im rechten Bereich auf die Schaltfläche **Eigenschaften**
   - Zeigen Sie die Eigenschaften des Objekts an, auf das das Richtlinienobjekt angewandt wird, und ändern Sie sie: Klicken Sie auf die Verknüpfung **Eigenschaften** neben der Bezeichnung **Angewendet auf**.

Der Befehl **Richtlinie prüfen** für ein Richtlinienobjekt führt eine Überprüfung für alle Objekte durch, die im Richtlinienbereich des Richtlinienobjekts gefunden wurden. Verwenden Sie den Befehl **Richtlinie prüfen** für ein Richtlinienobjekt, um alle Objekte zu suchen, die nicht den von diesem Richtlinienobjekt definierten Richtlinien entsprechen.

Deprovisionieren von Benutzern oder Gruppen

Die Quest One ActiveRoles-Benuterschnittstellen, sowohl die Quest One ActiveRoles-Konsole und das Web-Interface, stellen den Befehl **Deprovisionierung** für Benutzer- und Gruppenobjekte bereit. Dieser Befehl generiert eine Deprovisionsanforderung für die ausgewählten Objekte. Beim Verarbeiten der Anforderung führt Quest One ActiveRoles alle Vorgänge aus, die von den Deprovisionsrichtlinien vorgeschrieben werden.

Standardoptionen für die Deprovisionierung

Quest One ActiveRoles Enthält standardmäßig zwei integrierte Richtlinienobjekte, die die Vorgänge angeben, die bei der Deprovisionierung eines Benutzers oder einer Gruppe ausgeführt werden sollen. Diese Richtlinienobjekte finden Sie in der Quest One ActiveRoles-Konsole, indem Sie den Container **Configuration | Policies | Administration | Builtin** auswählen.

Das Richtlinienobjekt **Built-in Policy – User Default Deprovisioning** legt die standardmäßigen Auswirkungen des Befehls **Deprovisionierung** auf Benutzerkonten fest; das Richtlinienobjekt **Built-in Policy – Group Default Deprovisioning** legt die standardmäßigen Auswirkungen dieses Befehls auf Gruppen fest. Beide Objekte werden auf den Container **Active Directory** angewandt und wirken sich daher auf alle Domänen aus, die bei Quest One ActiveRoles registriert sind.

Die folgenden Tabellen fassen die Optionen der Standard-Deprovisionierungsrichtlinie zusammen. Wenn Sie die Deprovisionsrichtlinien nicht hinzufügen, entfernen oder ändern, führt Quest One ActiveRoles den Befehl **Deprovisionierung** für einen Benutzer oder eine Gruppe anhand dieser Optionen aus.

Standard-Deprovisionierungsrichtlinienoptionen für Benutzer, definiert durch das Richtlinienobjekt **Built-in Policy – User Default Deprovisioning**:

POLICY	OPTIONEN
Benutzerkonto-Deprovisionierung	• Benutzerkonto deaktivieren • Kennwort des Benutzers in einen willkürlichen Wert ändern • Ändern des Benutzernamens, sodass er das Deprovisionierungssuffix und das Datum der Deprovisionierung dieses Benutzers enthält • Ausfüllen der Benutzerbeschreibung, um anzuzeigen, dass dieses Benutzerkonto deprovisioniert wurde • Löschen bestimmter Eigenschaften des Benutzerkontos, wie Stadt, Firma und Adresse
Entfernung der Gruppenmitgliedschaft	• Entfernen des Benutzerkontos aus allen Sicherheitsgruppen • Entfernen des Benutzerkontos aus allen Verteilergruppen
Exchange-Postfach-Deprovisionierung	• Benutzerpostfach in der Exchange-Adressliste ausblenden, um so den Zugriff auf das Postfach zu verhindern
Stammordner-Deprovisionierung	• Aufheben des Zugriffs auf den Benutzerstammordner über das Benutzerkonto • Gewähren von Lesezugriff auf den Stammordner des Benutzers an den Vorgesetzten des Benutzers • Festlegen der Administratorengruppe als Besitzer des Stammordners
Benutzerkonto-Verschiebung	• Belassen des Benutzerkontos in der Organisationseinheit, in der es sich zum Zeitpunkt der Deprovisionierung befand
Permanentes Löschen des Benutzerkontos	• Verhindern der Löschung des Benutzerkontos

Standard-Deprovisionierungsrichtlinienoptionsen für Gruppen, definiert durch das Richtlinienobjekt **Built-in Policy – Group Default Deprovisioning**:

POLICY	OPTIONEN
Gruppenobjekt-Deprovisionierung	• Gruppentyp von „Sicherheit" in „Verteilung" ändern • Gruppe in der globalen Adressliste (GAL) ausblenden • Ändern des Gruppennamens, sodass er das Deprovisionierungssuffix und das Datum der Deprovisionierung dieser Gruppe enthält • Alle Mitglieder aus der Gruppe entfernen • Ausfüllen der Gruppenbeschreibung, um anzuzeigen, dass diese Gruppe deprovisioniert wurde
Gruppenobjekt-Verschiebung	• Belassen der Gruppe in der Organisationseinheit, in der sie sich zum Zeitpunkt der Deprovisionierung befand
Dauerhaftes Löschen des Gruppenobjekts	• Verhindern der Löschung der Gruppe

Delegieren der Deprovisionsaufgabe

Das Recht zur Deprovisionierung besitzt standardmäßig das Administratorkonto „ActiveRoles Server Admin", das während der Installation von Quest One ActiveRoles angegeben wird. Die Deprovisionierungsaufgabe kann jedoch an jeden beliebigen Benutzer und an jede beliebige Gruppe delegiert werden. Es wird eine ausschließlich für diesen Zweck vorgesehene Zugriffsvorlage bereitgestellt, damit Sie die Verwendung des Befehls **Deprovisionierung** delegieren können, ohne zugleich die Rechte für den Erstellungs- oder Löschvorgang zu delegieren.

Um die Deprovisionierung für Benutzer oder Gruppen in einem bestimmten Container (z.B. in einer Organisationseinheit oder einer verwalteten Einheit) zu delegieren, wenden Sie die Zugriffsvorlage wie folgt an:

Gehen Sie folgendermaßen vor, um die Deprovisionsaufgabe zu delegieren:

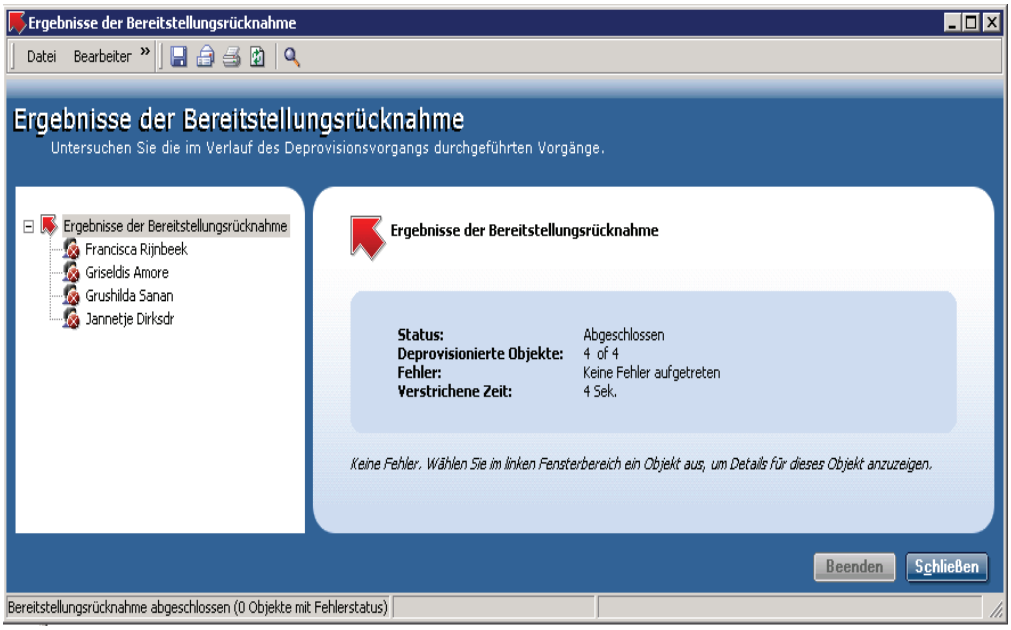
1. Klicken Sie in der Quest One ActiveRoles-Konsole mit der rechten Maustaste auf den Container und dann auf **Kontrolle delegieren**, um das Fenster **Quest One ActiveRoles-Sicherheit** anzuzeigen.
2. Klicken Sie im Fenster **Quest One ActiveRoles-Sicherheit** auf **Hinzufügen**, um den Assistenten zum Delegieren der Kontrolle zu starten. Klicken Sie auf **Weiter**.
3. Klicken Sie auf der Seite **Benutzer oder Gruppen** auf **Hinzufügen** und wählen Sie dann die Benutzer oder Gruppen aus, an die Sie die Rechte für Deprovisionsaufgabe delegieren möchten. Klicken Sie auf **Weiter**.
4. Erweitern Sie auf der Seite **Zugriffsvorlagen** den Ordner **Active Directory** und gehen Sie dann wie folgt vor:
   - Um die Aufgabe der Deprovisionierung von Benutzern zu delegieren, aktivieren Sie das Kontrollkästchen neben **Users – Perform Deprovisionierung Tasks**.
   - Um die Aufgabe der Deprovisionierung von Gruppen zu delegieren, aktivieren Sie das Kontrollkästchen neben **Groups – Perform Deprovisionierung Tasks**.
5. Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen im Assistenten; übernehmen Sie bei diesem Vorgang die Standardeinstellungen.

Nachdem Sie diese Schritte abgeschlossen haben, sind die in Schritt 3 ausgewählten Benutzer und Gruppen autorisiert, Benutzer und Gruppen in dem in Schritt 1 ausgewählten Container und ggf. in allen seinen Untercontainern zu deprovisionieren.

Verwenden des Deprovisionsbefehls

Der Befehl **Deprovisionierung** ist in der Quest One ActiveRoles-Konsole und im Web-Interface verfügbar. Mit dem Befehl **Deprovisionierung** starten Sie den Deprovisionierungsvorgang für die ausgewählten Objekte.

Der Fortschritt und die Ergebnisse des Vorgangs werden im Fenster **Ergebnisse der Bereitstellungsrücknahme** angezeigt. Nach Abschluss des Vorgangs wird in dem Fenster die Vorgangszusammenfassung angezeigt, sodass Sie die Vorgangsergebnisse detailliert untersuchen können. Die folgende Abbildung zeigt eine typische Vorgangszusammenfassung.



Im linken Bereich werden die deprovisionierten Objekte aufgelistet. Im rechten Bereich werden der Vorgangsstatus und ggf. die Fehlermeldungen angezeigt.

Um Vorgangsergebnisse anzuzeigen, wählen Sie im linken Bereich ein Objekt aus. Der rechte Bereich zeigt einen Bericht mit Informationen zu allen Aktionen, die während der Deprovisionierung des ausgewählten Objekts ausgeführt wurden. Im nächsten Abschnitt wird ein beispielhafter Bericht erörtert.

Bericht zu Ergebnissen der Deprovisionierung

Für jedes deprovisionierte Objekt können Sie im Fenster **Ergebnisse der Bereitstellungsrücknahme** die Ergebnisse des Deprovisionierungsvorgangs für dieses Objekt untersuchen.

Die Quest One ActiveRoles-Konsole oder das Web-Interface öffnet das Fenster **Ergebnisse der Deprovisionierung**, wenn der Befehl **Deprovisionierung** ausgeführt wird. Sie können dieses Fenster auch mit Hilfe des Befehls **Ergebnisse der Bereitstellungsrücknahme** öffnen, der für deprovisionierte Objekte verfügbar ist.

Im Fenster **Ergebnisse der Bereitstellungsrücknahme** wird ein Bericht über den Deprovisionierungsvorgang angezeigt. In dem Bericht sind Vorgangsergebnisse in Abschnitte gegliedert, die nach Richtlinienkategorien benannt sind. Jeder Abschnitt enthält Berichtselemente, die zu einer bestimmten Richtlinienkategorie gehören. Wenn Sie oben im Bericht auf die Überschrift klicken, wird der Bericht vollständig erweitert, und alle Berichtselemente werden angezeigt. Sie können auch einzelne Abschnitte in dem Bericht erweitern oder ausblenden, indem Sie auf die Überschrift des jeweiligen Berichts klicken.

Für bestimmte Elemente steht im Bericht die Option zur Verfügung, die Ansicht weiter zu erweitern und zusätzliche Informationen anzuzeigen. Durch Anklicken der Option **Liste** wird eine Liste von Elementen (z.B. Benutzer- oder Gruppeneigenschaften) anzeigen, die an dem Vorgang beteiligt sind. Indem Sie auf die Option **Details** klicken, können Sie das Vorgangsergebnis detaillierter untersuchen.

Das Fenster **Ergebnisse der Bereitstellungsrücknahme** erfüllt auch einige häufige Berichterstattungsanforderungen, einschließlich der Möglichkeit, alle Vorgangsergebnisse zum Drucken oder Anzeigen in einer Datei zu dokumentieren. Mit dem Kontextmenü können Sie den Bericht in eine Datei im HTML- oder XML-Format exportieren, ihn drucken oder über E-Mail versenden.

Berichtsinhalt

In den folgenden Tabellen sind die möglichen Berichtselemente aufgelistet. Es ist eine Tabelle pro Berichtsabschnitt vorhanden. Die Elemente in den einzelnen Abschnitten beschreiben Ergebnisse von den Aktionen, die in Übereinstimmung mit der entsprechenden Deprovisionierungsrichtlinie ausgeführt wurden. Berichtselemente enthalten außerdem Informationen zum Erfolg oder Fehler jeder Aktion. Bei einem Fehler enthält das Berichtselement eine Fehlerbeschreibung.

Nicht alle aufgelisteten Elemente müssen notwendigerweise in einem Bericht enthalten sein. Ein tatsächlicher Bericht enthält nur die Berichtselemente, die den konfigurierten Richtlinienoptionen entsprechen. Wenn die Richtlinie beispielsweise nicht für das Deaktivieren von Benutzerkonten konfiguriert ist, schließt der Bericht das Element zu dieser Aktion nicht ein.

Berichtsabschnitt: Benutzerkonto-Deprovisionierung

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Das Benutzerkonto ist deaktiviert.	Das Benutzerkonto konnte nicht deaktiviert werden.
Das Benutzerkennwort wird auf einen Zufallswert zurückgesetzt.	Zurücksetzen des Benutzerkennworts fehlgeschlagen.
Der Benutzeranmeldename wird in einen Zufallswert geändert.	Der Benutzeranmeldename konnte nicht geändert werden.
Der Benutzeranmeldename (Prä-Windows 2000) wird in einen Zufallswert geändert.	Der Benutzeranmeldename (vor Windows 2000) konnte nicht geändert werden.
Der Benutzername wurde geändert. Ursprünglicher Name: *Name* Neuer Name: *Name*	Der Benutzername konnte nicht geändert werden. Aktueller Name: *Name* Der folgende Name konnte nicht festgelegt werden: *Name*
Die Benutzereigenschaften werden geändert. Liste: • *Benutzereigenschaften, alte und neue Eigenschaftswerte*	Die Benutzereigenschaften konnten nicht geändert werden. Liste: • *Benutzereigenschaften, Fehlerbeschreibung*

Berichtsabschnitt: Entfernung der Gruppenmitgliedschaft

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Der Benutzer wird in Übereinstimmung mit der Richtlinie nicht aus Sicherheitsgruppen entfernt (Ausnahme: dynamische Gruppen und von einer Gruppenfamilie kontrollierte Gruppen). Details: • *Sicherheitsgruppen, zu denen der Benutzer gehört*	*Nicht zutreffend*
Der Benutzer wird aus allen Sicherheitsgruppen entfernt. Details: • *Sicherheitsgruppen, aus denen der Benutzer entfernt wird*	Der Benutzer konnte aus einigen Sicherheitsgruppen nicht entfernt werden. Details: • *Sicherheitsgruppen, aus denen der Benutzer entfernt wird* • *Sicherheitsgruppen, aus denen der Benutzer aufgrund eines Fehlers nicht entfernt wird*
In Übereinstimmung mit der Richtlinie verbleibt der Benutzer in einigen Sicherheitsgruppen. Details: • *Sicherheitsgruppen, aus denen der Benutzer entfernt wird* • *Sicherheitsgruppen, aus denen der Benutzer in Übereinstimmung mit der Richtlinie nicht entfernt wird*	Der Benutzer konnte aus einigen Sicherheitsgruppen nicht entfernt werden. Details: • *Sicherheitsgruppen, aus denen der Benutzer entfernt wird* • *Sicherheitsgruppen, aus denen der Benutzer in Übereinstimmung mit der Richtlinie nicht entfernt wird* • *Sicherheitsgruppen, aus denen der Benutzer aufgrund eines Fehlers nicht entfernt wird*
Der Benutzer wird in Übereinstimmung mit der Richtlinie nicht aus Verteilergruppen oder E-Mail-fähigen Sicherheitsgruppen entfernt (Ausnahme: dynamische Gruppen und von einer Gruppenfamilie kontrollierte Gruppen). Details: • *Verteilergruppen und E-Mail-fähige Sicherheitsgruppen, zu denen der Benutzer gehört*	*Nicht zutreffend*

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Der Benutzer wird aus allen Verteilergruppen und E-Mail-fähigen Sicherheitsgruppen entfernt. Details: • *Verteilergruppen und E-Mail-fähige Sicherheitsgruppen, aus denen der Benutzer entfernt wird*	Der Benutzer konnte aus einigen Verteilergruppen oder E-Mail-fähigen Sicherheitsgruppen nicht entfernt werden. Details: • *Verteilergruppen und E-Mail-fähige Sicherheitsgruppen, aus denen der Benutzer entfernt wird* • *Verteilergruppen oder E-Mail-fähige Sicherheitsgruppen, aus denen der Benutzer aufgrund eines Fehlers nicht entfernt wird*
In Übereinstimmung mit der Richtlinie verbleibt der Benutzer in einigen Verteilergruppen oder E-Mail-fähigen Sicherheitsgruppen. Details: • *Verteilergruppen und E-Mail-fähige Sicherheitsgruppen, aus denen der Benutzer entfernt wird* • *Verteilergruppen oder E-Mail-fähige Sicherheitsgruppen, aus denen der Benutzer in Übereinstimmung mit der Richtlinie nicht entfernt wird*	Der Benutzer konnte aus einigen Verteilergruppen oder E-Mail-fähigen Sicherheitsgruppen nicht entfernt werden. Details: • *Verteilergruppen und E-Mail-fähige Sicherheitsgruppen, aus denen der Benutzer entfernt wird* • *Verteilergruppen oder E-Mail-fähige Sicherheitsgruppen, aus denen der Benutzer in Übereinstimmung mit der Richtlinie nicht entfernt wird* • *Verteilergruppen oder E-Mail-fähige Sicherheitsgruppen, aus denen der Benutzer aufgrund eines Fehlers nicht entfernt wird*

Berichtsabschnitt: Exchange-Postfach-Deprovisionierung

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Die Deprovisionierung des Postfachs wird übersprungen, da der Benutzer nicht über ein Exchange-Postfach verfügt.	*Nicht zutreffend*
Das Benutzerpostfach wird aus der Globalen Adressliste (GAL) entfernt (ausgeblendet).	Das Benutzerpostfach konnte nicht aus der Globalen Adressliste (GAL) entfernt (ausgeblendet) werden.
Das Benutzerpostfach wird zur Unterdrückung von Nichtzustellbarkeitsberichten konfiguriert.	Das Benutzerpostfach konnte nicht für die Unterdrückung von Nichtzustellbarkeitsberichten konfiguriert werden.
Dem Vorgesetzten des Benutzers wird ein Vollzugriff auf das Benutzerpostfach gewährt. Name des Vorgesetzten: *Name*	Dem Vorgesetzten des Benutzers konnte kein Zugriff auf das Benutzerpostfach gewährt werden. Name des Vorgesetzten: *Name*
Nicht zutreffend	Dem Vorgesetzten des Benutzers konnte kein Zugriff auf das Benutzerpostfach gewährt werden. Grund: Der Vorgesetzte des Benutzers ist nicht im Verzeichnis angegeben.
Den erforderlichen Benutzern und Gruppen wurde Vollzugriff auf das Benutzerpostfach gewährt. Liste: • *Benutzer und Gruppen*	Den erforderlichen Benutzern und Gruppen konnte kein Zugriff auf das Benutzerpostfach gewährt werden. Liste: • *Benutzer und Gruppen*
Die Weiterleitung von Nachrichten an alternative Empfänger ist für das Benutzerpostfach nicht zulässig.	Die Weiterleitung von Nachrichten an alternative Empfänger konnte für das Benutzerpostfach nicht verweigert werden.

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Das Benutzerpostfach ist für die Weiterleitung eingehender Nachrichten an den Benutzerverwalter konfiguriert.	Das Benutzerpostfach konnte nicht für die Weiterleitung eingehender Nachrichten an den Benutzerverwalter konfiguriert werden.
Das Benutzerpostfach ist für die Weiterleitung eingehender Nachrichten an den Benutzerverwalter mit der Option, Kopien der Nachricht im Postfach zu belassen, konfiguriert.	Das Benutzerpostfach konnte nicht für die Weiterleitung eingehender Nachrichten an den Benutzerverwalter konfiguriert werden.
Das Benutzerpostfach konnte nicht für die Weiterleitung eingehender Nachrichten an den Benutzerverwalter konfiguriert werden. Grund: Der Vorgesetzte des Benutzers ist nicht im Verzeichnis angegeben.	*Nicht zutreffend*

Berichtsabschnitt: Stammordner-Deprovisionierung

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Die Deprovisionierung des Stammordners wird übersprungen, da der Benutzer nicht über einen Stammordner verfügt.	*Nicht zutreffend*
Die Rechte des Benutzers für den Stammordner werden entfernt.	Die Rechte des Benutzers für den Stammordner konnten nicht entfernt werden.
Dem Vorgesetzten des Benutzers wird Lesezugriff auf den Stammordner des Benutzers gewährt. Name des Vorgesetzten: *Name*	Dem Vorgesetzten des Benutzers konnte kein Lesezugriff auf den Stammordner des Benutzers gewährt werden. Name des Vorgesetzten: *Name*
Nicht zutreffend	Dem Vorgesetzten des Benutzers konnte kein Lesezugriff auf den Stammordner des Benutzers gewährt werden. Grund: Der Vorgesetzte des Benutzers ist nicht im Verzeichnis angegeben.
In Übereinstimmung mit der Richtlinie wird beim Löschen des Benutzerkontos auch der Stammordner gelöscht. Name des Stammordners: *Name*	*Nicht zutreffend*
Den erforderlichen Benutzern und Gruppen wurde Lesezugriff auf den Stammordner des Benutzers gewährt. Liste: • *Benutzer und Gruppen*	Den erforderlichen Benutzern und Gruppen konnte kein Lesezugriff auf den Stammordner des Benutzers gewährt werden. Liste: • *Benutzer und Gruppen*
Dem Stammordner des Benutzers wird ein neuer Eigentümer zugewiesen. Name des Besitzers *Name*	Dem Stammordner des Benutzers konnte kein neuer Besitzer zugewiesen werden. Dieser Besitzername konnte nicht festgelegt werden: *Name*

Berichtsabschnitt: Benutzerkonto-Verschiebung

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Das Benutzerkonto wird in Übereinstimmung mit der Richtlinie nicht von seinem ursprünglichen Speicherort verschoben: *Name des Containers*	*Nicht zutreffend*
Das Benutzerkonto wird an einen anderen Speicherort verschoben. Ursprünglicher Speicherort: *Name des Containers* Neuer Speicherort: *Name des Containers*	Das Benutzerkonto konnte nicht an einen anderen Speicherort verschoben werden. Ursprünglicher Speicherort: *Name des Containers* Das Verschieben an diesen Speicherort ist fehlgeschlagen: *Name des Containers*

Berichtsabschnitt: Permanentes Löschen des Benutzerkontos

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
In Übereinstimmung mit der Richtlinie wird das Löschen des Benutzerkontos nicht geplant.	*Nicht zutreffend*
Das Löschen des Benutzerkontos wird im Zeitplan festgelegt. Wird gelöscht an folgendem Datum: *Datum*	Die Löschung des Benutzerkontos konnte nicht geplant werden.
Das Benutzerkonto wurde in den Active Directory-Papierkorb verschoben.	Das Benutzerkonto konnte nicht in den Active Directory-Papierkorb verschoben werden. Überprüfen Sie, ob der Active Directory-Papierkorb aktiviert ist.

Berichtsabschnitt: Gruppenobjekt-Deprovisionierung

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Der Gruppentyp wurde von „Sicherheit" in „Verteilung" geändert.	Der Gruppentyp konnte nicht von „Sicherheit" in „Verteilung" geändert werden.
Der Gruppentyp kann nicht von „Sicherheit" in „Verteilung" geändert werden, weil die Gruppe keine Sicherheitsgruppe ist.	*Nicht zutreffend*
Die Gruppe wurde aus der globalen Adressliste (GAL) entfernt (ausgeblendet).	Die Gruppe konnte nicht aus der globalen Adressliste (GAL) entfernt (ausgeblendet) werden.
Die Gruppe kann nicht aus der globalen Adressliste (GAL) entfernt (ausgeblendet) werden, weil dies keine E-Mail-fähige Gruppe ist.	*Nicht zutreffend*
Der Gruppenname wurde geändert. Ursprünglicher Name: *Name* Neuer Name: *Name*	Der Gruppenname konnte nicht geändert werden. Aktueller Name: *Name* Der folgende Name konnte nicht festgelegt werden: *Name*
In Übereinstimmung mit der Richtlinie werden die Mitglieder nicht aus der Gruppe entfernt. Details: • *Liste der in der Gruppe beibehaltenen Mitglieder*	*Nicht zutreffend*

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Die Mitglieder sind aus der Gruppe entfernt. Details: • *Liste der aus der Gruppe entfernten Mitglieder*	Einige Mitglieder konnten nicht aus der Gruppe entfernt werden. Details: • *Liste der aus der Gruppe entfernten Mitglieder* • *Liste der Mitglieder, die aufgrund eines Fehlers nicht aus der Gruppe entfernt wurden*
In Übereinstimmung mit der Richtlinie bleiben einige Mitglieder in der Gruppe. Details: • *Liste der aus der Gruppe entfernten Mitglieder* • *Liste der in der Gruppe beibehaltenen Mitglieder*	Einige Mitglieder konnten nicht aus der Gruppe entfernt werden. Details: • *Liste der aus der Gruppe entfernten Mitglieder* • *Liste der Mitglieder, die in Übereinstimmung mit der Richtlinie in der Gruppe beibehalten wurden* • *Liste der Mitglieder, die aufgrund eines Fehlers nicht aus der Gruppe entfernt wurden*
Die Gruppeneigenschaften wurden geändert. Liste: • *Eigenschaftsnamen, alte und neue Eigenschaftswerte*	Die Gruppeneigenschaften konnten nicht geändert werden. Liste: • *Eigenschaftsnamen, Fehlerbeschreibung*

Berichtsabschnitt: Gruppenobjekt-Verschiebung

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Die Gruppe wird in Übereinstimmung mit der Richtlinie nicht von ihrem ursprünglichen Speicherort verschoben: *Name des Containers*	*Nicht zutreffend*
Die Gruppe wird an einen anderen Speicherort verschoben. Ursprünglicher Speicherort: *Name des Containers* Neuer Speicherort: *Name des Containers*	Die Gruppe konnte nicht an einen anderen Speicherort verschoben werden. Ursprünglicher Speicherort: *Name des Containers* Das Verschieben an diesen Speicherort ist fehlgeschlagen: *Name des Containers*

Berichtsabschnitt: Dauerhaftes Löschen des Gruppenobjekts

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
In Übereinstimmung mit der Richtlinie wird das Löschen der Gruppe nicht geplant.	*Nicht zutreffend*
Das Löschen der Gruppe wird im Zeitplan festgelegt. Wird gelöscht an folgendem Datum: *Datum*	Die Löschung der Gruppe konnte nicht geplant werden.
Die Gruppe wurde in den Active Directory-Papierkorb verschoben.	Die Gruppe konnte nicht in den Active Directory-Papierkorb verschoben werden. Überprüfen Sie, ob der Active Directory-Papierkorb aktiviert ist.

Berichtsabschnitt: Benachrichtigungsverteilung

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Die Deprovisionierungsbenachrichtigung wird an die aufgeführten Empfänger gesendet (bisher nicht gesendet). Liste: • *Empfänger*	*Nicht zutreffend*
Die Deprovisionierungsbenachrichtigung wurde an die aufgeführten Empfänger gesendet. Liste: • *Empfänger*	Aufgrund eines Fehlers wurde keine Deprovisionierungsbenachrichtigung an die aufgeführten Empfänger gesendet. Liste: • *Empfänger*

Berichtsabschnitt: Berichtsverteilung

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Der Deprovisionierungsbericht wird nicht gesendet, da keine Fehler aufgetreten sind.	*Nicht zutreffend*
Der Deprovisionierungsbericht wird an die aufgeführten Empfänger gesendet (bisher nicht gesendet). Liste: • *Empfänger*	*Nicht zutreffend*
Der Deprovisionierungsbericht wurde an die aufgeführten Empfänger gesendet. Liste: • *Empfänger*	Aufgrund eines Fehlers wurde der Deprovisionierungsbericht nicht an die aufgeführten Empfänger gesendet. Liste: • *Empfänger*

Wiederherstellen von deprovisionierten Benutzern oder Gruppen

Quest One ActiveRoles Bietet die Möglichkeit, deprovisionierte Objekte wie etwa deprovisionierte Benutzer oder Gruppen wiederherzustellen. Der Zweck dieses Vorgangs, der als *Aufhebung der Deprovisionierung* bezeichnet wird, besteht darin, die Änderungen rückgängig zu machen, die durch den Deprovisionierungsvorgang an einem Objekt vorgenommen wurden. Wenn ein deprovisioniertes Objekt wiederhergestellt werden muss (zum Beispiel wenn ein Benutzerkonto versehentlich deprovisioniert wurde), ermöglicht der Vorgang „Deprovisionierung aufheben", das Objekt schnell wieder in den Zustand zurückzuversetzen, in dem es sich befand, bevor die Änderungen vorgenommen wurden.

Durch die Aufhebung der Deprovisionierung werden die Änderungen rückgängig gemacht, die in Übereinstimmung mit der Standard-Deprovisionierungsrichtlinie am Objekt vorgenommen wurden. Gehen wir zum Beispiel einmal davon aus, dass eine Benutzerkonto-Deprovisionierungsrichtlinie so konfiguriert ist, dass ein deprovisioniertes Benutzerkonto folgende Merkmale aufweist:

- Das Benutzerkonto ist deaktiviert
- Das Benutzerkonto ist umbenannt
- Die Beschreibung des Benutzerkontos ist geändert
- Das Benutzerkonto verfügt über eine Reihe von deaktivierten Eigenschaften
- Das Kennwort des Benutzerkontos ist auf einen zufälligen Wert gesetzt

In diesem Fall führt die Aufhebung des Deprovisionierungsvorgangs dazu, dass:

- Das Benutzerkonto wieder die folgenden Merkmale aufweist
- Die Beschreibung, der Name und andere Eigenschaften werden wieder auf die ursprünglichen Werte des Benutzerkontos zurückgesetzt
- Das Benutzerkonto bietet die Option, das Kennwort zurückzusetzen, sodass sich der Benutzer anmelden kann

Ein ähnliches Verhalten gilt für andere Richtlinien der Deprovisionierungskategorie:

- Wenn der Deprovisionierungsvorgang den Benutzerzugriff auf Ressourcen wie etwa den Stammordner oder das Exchange-Postfach aufhebt, dann versucht die Aufhebung des Deprovisionierungsvorgangs, den Benutzerzugriff auf diese Ressourcen wiederherzustellen.
- Wenn der Deprovisionierungsvorgang ein Benutzerkonto aus bestimmten Gruppen entfernt, dann kann die Aufhebung des Deprovisionierungsvorgang das Benutzerkonto zu diesen Gruppen hinzufügen und somit die Original-Gruppenmitgliedschaften des Benutzerkontos wiederherstellen.

Um ein weiteres Beispiel anzuführen, gehen wir davon aus, dass die Deprovisionierungsrichtlinie so konfiguriert ist, dass ein Deprovisionierungsvorgang für eine Gruppe:

- alle Mitglieder aus der Gruppe entfernt
- die Gruppe umbenennt
- die Gruppe in einen bestimmten Container verschiebt

In diesem Fall führt die Aufhebung des Deprovisionierungsvorgangs dazu, dass:

- die ursprüngliche Mitgliedschaftsliste der Gruppe in den Zustand zurückversetzt wird, den sie zum Zeitpunkt der Deprovisionierung aufwies.
- die Gruppe umbenannt wird, wobei der ursprüngliche Name der Gruppe wiederhergestellt wird.
- die Gruppe in den Container verschoben wird, in dem sich die Gruppe zum Zeitpunkt der Deprovisionierung befunden hat.

Ein ähnliches Verhalten gilt für andere Optionen der Richtlinie zur Deprovisionierung von Gruppen:

- Wenn der Deprovisionierungsvorgang die Gruppe in der Globalen Adressliste (GAL) ausblendet, stellt der Befehl „Deprovisionierung aufheben" die Sichtbarkeit der Gruppe in der GAL wieder her.
- Wenn der Deprovisionierungsvorgang den Gruppentyp von „Sicherheit" in „Verteilung" ändert, setzt der Befehl „Deprovisionierung aufheben" den Gruppentyp auf „Sicherheit" zurück.
- Wenn der Deprovisionierungsvorgang jegliche andere Eigenschaften der Gruppe ändert, stellt der Befehl „Deprovisionierung aufheben" die ursprünglichen Eigenschaftswerte wieder her.

Sowohl die Quest One ActiveRoles-Konsole als auch das Web-Interface stellen den Befehl **Deprovisionierung aufheben** für deprovisionierte Benutzer oder Gruppen bereit. Wenn dieser Befehl für ein deprovisioniertes Objekt ausgewählt wird, sendet er eine Anforderung zur Wiederherstellung des Objekts. Bei Erhalt der Anforderung führt Quest One ActiveRoles alle erforderlichen Vorgänge durch, um die Ergebnisse der Deprovisionierung des Objekts rückgängig zu machen, und erstellt einen detaillierten Bericht über die durchgeführten Vorgänge. Dieser Bericht enthält außerdem Informationen über den Erfolg oder Misserfolg jedes Vorgangs.

Richtlinienoptionen für die Aufhebung der Deprovisionierung eines Benutzers

Das Verhalten des Vorgangs „Deprovisionierung aufheben" wird durch eine konfigurierbare Richtlinie bestimmt, die in einem integrierten Richtlinienobjekt enthalten ist. Hierbei handelt es sich um das Richtlinienobjekt mit dem Namen **Built-in Policy – Default Rules to Undo User Deprovisioning**. Siebefindet sich im Container **Builtin** unter **Configuration/Policies/Administration**. Das Richtlinienobjekt wird auf den Ordner **Active Directory** angewendet und wirkt sich daher auf alle Domänen aus, die bei Quest One ActiveRoles registriert sind (verwaltete Domänen).

Die von dieser Richtlinie bereitgestellte Option kann verwendet werden, um die Wiederherstellung von Gruppenmitgliedschaften und das Rücksetzen des Benutzerkennworts zu verhindern:

- **Gruppenmitgliedschaften wiederherstellen.** Bei Auswahl dieser Option führt die Aufhebung des Deprovisionierungsvorgangs für ein deprovisioniertes Benutzerkonto zum Hinzufügen des Kontos zu den Verteiler- und Sicherheitsgruppen, aus denen das Konto in Übereinstimmung mit der Richtlinie zum Entfernen von Gruppenmitgliedschaften entfernt wurde. Wenn Sie nicht möchten, dass wiederhergestellte Konten automatisch zu Gruppen hinzugefügt werden, dann deaktivieren Sie diese Option.

  Beachten Sie, dass Quest One ActiveRoles unabhängig davon, ob diese Option aktiviert oder deaktiviert ist, nach der Wiederherstellung eines deprovisionierten Benutzerkontos das Konto abhängig von seinen Eigenschaften automatisch zu den entsprechenden dynamischen Gruppen und Gruppenfamilien hinzufügt.

- **Kennwort unverändert lassen.** Führt dazu, dass die Aufhebung des Deprovisionierungsvorgangs für ein deprovisioniertes Benutzerkonto das Rücksetzen des Kennworts für das wiederhergestellte Konto verhindert. Aktivieren Sie diese Option, wenn Sie möchten, dass das Kennwort vom Help Desk oder mit Hilfe einer Self-Service-Kennwortverwaltungslösung wiederhergestellt wird, nachdem das Konto wiederhergestellt wurde.
- **Zum Rücksetzen des Kennworts auffordern.** Führt dazu, dass die Aufhebung des Deprovisionierungsvorgangs für ein deprovisioniertes Benutzerkonto das Rücksetzen des Kennworts für das wiederhergestellte Konto ermöglicht. Wenn diese Option ausgewählt ist, zeigt der Befehl **Deprovisionierung aufheben** ein Dialogfeld an, in dem das Kennwort zurückgesetzt werden kann.

Gehen Sie folgendermaßen vor, um die Richtlinienoptionen anzuzeigen oder zu ändern:

1. Öffnen Sie die Quest One ActiveRoles-Konsole.
2. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Policies | Administration** und wählen Sie dann **Builtin** unter **Administration**
3. Doppelklicken Sie im Bereich „Details" auf **Built-in Policy – Default Rules to Undo User Deprovisioning**.
4. Klicken Sie auf der Registerkarte **Richtlinien** im Dialogfeld **Eigenschaften** auf die Richtlinie in der Liste und klicken Sie dann auf **Anzeigen/Bearbeiten**, um auf die Richtlinienoptionen zuzugreifen.

Da das integrierte Richtlinienobjekt normalerweise auf den Active Directory-Knoten im Quest One ActiveRoles-Namespace angewandt wird, gelten die Richtlinienoptionen für alle deprovisionierten Benutzerkonten. Wenn Sie verschiedene Richtlinienoptionen für unterschiedliche Domänen oder Container benötigen, erstellen Sie eine Kopie des integrierten Richtlinienobjekts, konfigurieren Sie dann die Kopie entsprechend und wenden Sie sie dann wie gewünscht an.

Der Vorgang „Deprovisionierung aufheben" ist normalerweise in allen bei Quest One ActiveRoles registrierten Domänen aktiviert. Es ist möglich, diesen Vorgang in einzelnen Domänen oder Containern oder in allen Domänen zu verhindern, indem Sie die Richtlinie sperren oder deaktivieren, die den Vorgang regelt. Bei Deaktivierung des integrierten Richtlinienobjekts kann eine aktivierte Kopie dieses Richtlinienobjekts angewandt werden, um den Vorgang „Deprovisionierung aufheben" in einzelnen Domänen oder Containern zu ermöglichen.

Delegieren der Aufhebung der Deprovisionierung

Das Recht zur Wiederherstellung von deprovisionierten Benutzern oder Gruppen besitzt standardmäßig das Administratorkonto „ActiveRoles Server Admin", das während der Installation von Quest One ActiveRoles angegeben wird. Diese Aufgabe kann jedoch an jede beliebigen Gruppe oder jeden beliebigen Benutzer delegiert werden. Es wird eine ausschließlich für diesen Zweck vorgesehene Zugriffsvorlage bereitgestellt, damit Sie die Verwendung des Befehls **Deprovisionierung aufheben** delegieren können, ohne zugleich die Rechte für den Erstellungs- oder Löschvorgang zu delegieren.

Um die Wiederherstellung deprovisionierter Benutzer oder Gruppen, die sich in einem bestimmten Container wie etwa in einer Organisationseinheit oder einer verwalteten Einheit befinden, zu delegieren, wenden Sie die Zugriffsvorlage wie folgt an:

Gehen Sie folgendermaßen vor, um die Aufhebung der Deprovisionierung zu delegieren:

1. Klicken Sie in der Quest One ActiveRoles-Konsole mit der rechten Maustaste auf den Container und dann auf **Kontrolle delegieren**, um das Fenster **Quest One ActiveRoles-Sicherheit** anzuzeigen.
2. Klicken Sie im Fenster **Quest One ActiveRoles-Sicherheit** auf **Hinzufügen**, um den Assistenten zum Delegieren der Kontrolle zu starten. Klicken Sie auf **Weiter**.
3. Klicken Sie auf der Seite **Benutzer oder Gruppen** auf **Hinzufügen** und wählen Sie dann die Benutzer oder Gruppen, an die Sie die Aufgabe delegieren möchten. Klicken Sie auf **Weiter**.
4. Erweitern Sie auf der Seite **Zugriffsvorlagen** den Ordner **Active Directory** und gehen Sie dann wie folgt vor:
   - Um die Aufgabe der Wiederherstellung von deprovisionierten Benutzern zu delegieren, aktivieren Sie das Kontrollkästchen neben **Users - Perform Undo Deprovisionierung Tasks**.
   - Um die Aufgabe der Wiederherstellung von deprovisionierten Gruppen zu delegieren, aktivieren Sie das Kontrollkästchen neben **Groups - Perform Undo Deprovisionierung Tasks**.
5. Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen im Assistenten; übernehmen Sie bei diesem Vorgang die Standardeinstellungen.

Nachdem Sie diese Schritte abgeschlossen haben, sind die in Schritt 3 ausgewählten Benutzer und Gruppen autorisiert, die Deprovisionierung von Benutzern in dem in Schritt 1 ausgewählten Container und ggf. in allen seinen Untercontainern zurückzunehmen.

Verwenden des Befehls zur Aufhebung der Deprovisionierung

Der Befehl **Deprovisionierung aufheben** steht über die Konsole und das Web-Interface von Quest One ActiveRoles denjenigen Benutzern zur Verfügung, die zum Wiederherstellen von deprovisionierten Benutzern oder Gruppen autorisiert sind. Bei Verwendung dieses Befehls starten Sie die Aufhebung des Deprovisionierungsvorgangs für die von Ihnen ausgewählten Objekte, wodurch Quest One ActiveRoles die Ergebnisse der Deprovisionierung dieser Objekte rückgängig macht.

Gehen Sie folgendermaßen vor, um ein deprovisioniertes Benutzerkonto wiederherzustellen:

1. Klicken Sie in der Quest One ActiveRoles-Konsole mit der rechten Maustaste auf das Benutzerkonto und klicken Sie dann auf **Deprovisionierung aufheben**.
2. Wählen Sie im Dialogfeld **Kennwortoptionen** die Optionen, die auf das Kennwort des wiederhergestellten Kontos angewandt werden sollen, und klicken Sie dann auf **OK**.

   *Für weitere Informationen zu jeder Option öffnen Sie das Dialogfeld **Kennwortoptionen** und drücken Sie dann auf F1.*
3. Warten Sie, während Quest One ActiveRoles das Benutzerkonto wiederherstellt.

Gehen Sie folgendermaßen vor, um eine deprovisionierte Gruppe wiederherzustellen:

1. Klicken Sie in der Quest One ActiveRoles-Konsole mit der rechten Maustaste auf die Gruppe und klicken Sie dann auf **Deprovisionierung aufheben**.
2. Warten Sie, während Quest One ActiveRoles die Gruppe wiederherstellt.

Der Fortschritt des Vorgangs und die Ergebnisse werden im Fenster **Ergebnisse der Aufhebung der Deprovisionierung** angezeigt, das dem weiter oben in diesem Kapitel beschriebenen Fenster **Ergebnisse der Bereitstellungsrücknahme** entspricht. Nach Abschluss des Vorgangs wird in dem Fenster die Vorgangszusammenfassung angezeigt, sodass Sie die Vorgangsergebnisse detailliert untersuchen können.

Bericht über die Ergebnisse der Aufhebung der Deprovisionierung

Für jedes wiederhergestellte Objekt können Sie im Fenster **Ergebnisse der Aufhebung der Deprovisionierung** die Ergebnisse des Wiederherstellungsvorgangs für dieses Objekt untersuchen. Die Quest One ActiveRoles-Konsole oder das Web-Interface öffnet das Fenster **Ergebnisse der Aufhebung der Deprovisionierung**, wenn der Befehl **Deprovisionierung aufheben** ausgeführt wird.

Im Fenster **Ergebnisse der Aufhebung der Deprovisionierung** wird ein Bericht über die Aufhebung des Deprovisionierungsvorgangs angezeigt, das dem weiter oben in diesem Kapitel beschriebenen, im Zusammenhang mit der Deprovisionierung stehenden Bericht entspricht. In dem Bericht sind Vorgangsergebnisse in Abschnitte gegliedert, wobei jeder Abschnitt Berichtselemente, die zu einer bestimmten Deprovisionierungsrichtlinienkategorie gehören, enthält. Die Berichtselemente innerhalb eines bestimmten Abschnitts geben Auskunft über die Vorgänge, die durchgeführt wurden, um die Änderungen rückgängig zu machen, die von der Deprovisionierungsrichtlinie der entsprechenden Kategorie vorgenommen wurden.

Wenn Sie oben im Bericht auf die Überschrift klicken, wird der Bericht vollständig erweitert, und alle Berichtselemente werden angezeigt. Sie können auch einzelne Abschnitte in dem Bericht erweitern oder ausblenden, indem Sie auf die Überschrift des jeweiligen Berichts klicken.

Für bestimmte Elemente steht im Bericht die Option zur Verfügung, die Ansicht weiter zu erweitern und zusätzliche Informationen anzuzeigen. Durch Anklicken der Option **Liste** wird eine Liste von Elementen (z.B. Benutzer- oder Gruppeneigenschaften) anzeigen, die an dem Vorgang beteiligt sind. Indem Sie auf die Option **Details** klicken, können Sie das Vorgangsergebnis detaillierter untersuchen.

Das Fenster **Ergebnisse der Aufhebung der Deprovisionierung** bietet auch die Möglichkeit, alle Vorgangsergebnisse in einer Datei für den Druck oder die Anzeige zu dokumentieren. Mit dem Kontextmenü können Sie den Bericht in eine Datei im HTML- oder XML-Format exportieren, ihn drucken oder über E-Mail versenden.

Berichtsinhalt

In den folgenden Tabellen sind die möglichen Berichtselemente aufgelistet. Es ist eine Tabelle pro Berichtsabschnitt vorhanden. Die Elemente in den einzelnen Abschnitten beschreiben die Ergebnisse der Aktionen, die ausgeführt wurden, um die von der entsprechenden Deprovisionierungsrichtlinie vorgenommenen Änderungen rückgängig zu machen. Berichtselemente enthalten außerdem Informationen zum Erfolg oder Fehler jeder Aktion. Bei einem Fehler enthält das Berichtselement eine Fehlerbeschreibung.

Nicht alle aufgelisteten Elemente müssen notwendigerweise in einem Bericht enthalten sein. Ein Bericht umfasst nur Berichtselemente, die in Zusammenhang mit den Deprovisionierungsrichtlinien stehen, die gültig waren, als der Benutzer oder die Gruppe deprovisioniert wurde.

Berichtsabschnitt: Benutzerkontodeprovisionierung aufheben

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Das Benutzerkonto ist aktiviert.	Das Benutzerkonto konnte nicht aktiviert werden.
Das Benutzerkennwort wird auf einen bekannten Wert mit den folgenden Kennwortoptionen zurückgesetzt: *<Liste der Optionen>*	Zurücksetzen des Benutzerkennworts fehlgeschlagen.
Das aktuelle Benutzerkennwort bleibt unverändert.	*Nicht zutreffend*
Der Benutzername wird wiederhergestellt. Alter Name: *Name* Wiederhergestellter Name: *Name*	Der Benutzername konnte nicht wiederhergestellt werden. Aktueller Name: *Name* Der folgende Name konnte nicht festgelegt werden: *Name*
Die Benutzereigenschaften werden wiederhergestellt. Liste: • *Benutzereigenschaften, neue Eigenschaftswerte*	Die Benutzereigenschaften konnten nicht wiederhergestellt werden. Liste: • *Benutzereigenschaften, Fehlerbeschreibung*

Berichtsabschnitt: Entfernen der Gruppenmitgliedschaft rückgängig machen

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
In Übereinstimmung mit der Richtlinie wird die Mitgliedschaft des Benutzers in Sicherheitsgruppen nicht wiederhergestellt.	*Nicht zutreffend*
In Übereinstimmung mit der Richtlinie wird die Mitgliedschaft des Benutzers in Verteilergruppen oder E-Mail-fähigen Sicherheitsgruppen nicht wiederhergestellt.	*Nicht zutreffend*
Die Mitgliedschaft des Benutzers in Sicherheitsgruppen wird wiederhergestellt. Details: • *Sicherheitsgruppen, zu denen der Benutzer hinzugefügt wird*	Die Mitgliedschaft des Benutzers in einigen Sicherheitsgruppen konnte nicht wiederhergestellt werden. Details: • *Sicherheitsgruppen, zu denen der Benutzer hinzugefügt wird* • *Sicherheitsgruppen, zu denen der Benutzer aufgrund eines Fehlers nicht hinzugefügt wird*
Die Mitgliedschaft des Benutzers in Verteilergruppen und E-Mail-fähigen Sicherheitsgruppen wird wiederhergestellt. Details: • *Verteilergruppen und E-Mail-fähige Sicherheitsgruppen, zu denen der Benutzer hinzugefügt wird*	Die Mitgliedschaft des Benutzers in einigen Verteilergruppen oder E-Mail-fähigen Sicherheitsgruppen konnte nicht wiederhergestellt werden. Details: • *Verteilergruppen und E-Mail-fähige Sicherheitsgruppen, zu denen der Benutzer hinzugefügt wird* • *Verteilergruppen oder E-Mail-fähige Sicherheitsgruppen, zu denen der Benutzer aufgrund eines Fehlers nicht hinzugefügt wird*

Berichtsabschnitt: Exchange-Postfach-Deprovisionierung aufheben

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Die Wiederherstellung des Benutzerpostfachs wird übersprungen, da der Benutzer zum Zeitpunkt der Deprovisionierung über kein Exchange-Postfach verfügte.	*Nicht zutreffend*
Der ursprüngliche Zustand des Benutzerpostfachs wird in der Globalen Adressliste (GAL) wiederhergestellt.	Der ursprüngliche Zustand des Benutzerpostfachs in der Globalen Adressliste (GAL) konnte nicht wiederhergestellt werden.
Die ursprünglichen Einstellungen für das Senden von Nichtzustellbarkeitsberichten werden für das Benutzerpostfach wiederhergestellt.	Die ursprünglichen Einstellungen für das Senden von Nichtzustellbarkeitsberichten konnten nicht für das Benutzerpostfach wiederhergestellt werden.
Die ursprüngliche Konfiguration der E-Mail-Weiterleitung für das Benutzerpostfach wird wiederhergestellt.	Die ursprüngliche Konfiguration der E-Mail-Weiterleitung für das Benutzerpostfach konnte nicht wiederhergestellt werden.
Die ursprünglichen Sicherheitseinstellungen werden im Benutzerpostfach wiederhergestellt.	Die ursprünglichen Sicherheitseinstellungen im Benutzerpostfach konnten nicht wiederhergestellt werden.

Berichtsabschnitt: Stammordner-Deprovisionierung aufheben

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Die Wiederherstellung des Stammordners wird übersprungen, da der Benutzer zum Zeitpunkt der Deprovisionierung über keinen Stammordner verfügte.	*Nicht zutreffend*
Die ursprünglichen Sicherheitseinstellungen werden im Stammordner des Benutzers wiederhergestellt.	Die ursprünglichen Sicherheitseinstellungen im Stammordner des Benutzers konnten nicht wiederhergestellt werden.

Berichtsabschnitt: Benutzerkonto-Verschiebung rückgängig machen

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Es wurden keine rückgängig zu machenden Änderungen vorgenommen.	*Nicht zutreffend*
Das Benutzerkonto wird an seinen ursprünglichen Speicherort verschoben. Ehemaliger Speicherort: *Name des Containers* Wiederhergestellter ursprünglicher Speicherort: *Name des Containers*	Das Benutzerkonto konnte nicht an seinen ursprünglichen Speicherort verschoben werden. Aktueller Speicherort: *Name des Containers* Das Verschieben an diesen Speicherort ist fehlgeschlagen: *Name des Containers*

Berichtsabschnitt: Permanentes Löschen des Benutzerkontos rückgängig machen

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Es wurden keine rückgängig zu machenden Änderungen vorgenommen.	*Nicht zutreffend*
Die geplante Löschung des Benutzerkontos wird abgebrochen.	Der Abbruch der geplanten Löschung des Benutzerkontos ist fehlgeschlagen. Das Konto wird an diesem Datum gelöscht: *Datum*

Berichtsabschnitt: Deprovisionierung des Gruppenobjekts rückgängig machen

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Der Gruppentyp wurde wieder in „Sicherheitsgruppe" zurück geändert.	Der Gruppentyp konnte nicht wieder in „Sicherheit" geändert werden.
Die Gruppe wurde in der globalen Adressliste (GAL) wiederhergestellt.	Die Gruppe konnte nicht in der globalen Adressliste (GAL) wiederhergestellt werden.
Der Gruppenname wird wiederhergestellt. Alter Name: *Name* Wiederhergestellter Name: *Name*	Der Gruppenname konnte nicht wiederhergestellt werden. Aktueller Name: *Name* Der folgende Name konnte nicht festgelegt werden: *Name*
Die Mitgliedschaftsliste der Gruppe ist wiederhergestellt. Details: • *Liste der zur Gruppe hinzugefügten Mitglieder*	Die Mitgliederliste der Gruppe konnte nicht wiederhergestellt werden. Details: • *Liste der zur Gruppe hinzugefügten Mitglieder* • *Liste der Mitglieder, die aufgrund eines Fehlers nicht zur Gruppe hinzugefügt wurden*
Die Gruppeneigenschaften wurden wiederhergestellt. Liste: • *Gruppeneigenschaften, neue Eigenschaftswerte*	Die Gruppeneigenschaften konnten nicht wiederhergestellt werden. Liste: • *Gruppeneigenschaften, Fehlerbeschreibung*

Berichtsabschnitt: Verschieben des Gruppenobjekts rückgängig machen

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Es wurden keine rückgängig zu machenden Änderungen vorgenommen.	*Nicht zutreffend*
Die Gruppe wird an ihren ursprünglichen Speicherort verschoben. Ehemaliger Speicherort: *Name des Containers* Wiederhergestellter ursprünglicher Speicherort: *Name des Containers*	Die Gruppe konnte nicht an ihren ursprünglichen Speicherort verschoben werden. Aktueller Speicherort: *Name des Containers* Das Verschieben an diesen Speicherort ist fehlgeschlagen: *Name des Containers*

Berichtsabschnitt: Dauerhaftes Löschen des Gruppenobjekts rückgängig machen

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Es wurden keine rückgängig zu machenden Änderungen vorgenommen.	*Nicht zutreffend*
Die geplante Löschung der Gruppe wurde abgebrochen.	Der Abbruch der geplanten Löschung der Gruppe ist fehlgeschlagen. Die Gruppe wird an diesem Datum gelöscht: *Datum*

Richtlinie zur Vermeidung einer Containerlöschung

Wenn ein Administrator ein Containerobjekt wie etwa eine Organisationseinheit, die über untergeordnete Objekte verfügt, auswählt und löscht, kann es zu einem Massenlöschvorgang kommen. Obwohl Massenlöschungen selten sind, sind dies Ereignisse, die zu einer Unterbrechung des Betriebs führen und gegen die Sie sich schützen können, indem Sie eine neue Richtlinie nutzen: der Containerlöschschutz.

Einer der am häufigsten vorkommenden Massenlöschvorgänge ist das Löschen eines Containers. Dieses Ereignis kann eintreten, wenn Quest One ActiveRoles verwendet wird, um ein Containerobjekt zu löschen, das andere (untergeordnete) Objekte enthält. Standardmäßig weist eine Containerlöschung die folgenden Merkmale auf:

- Zunächst erstellt Quest One ActiveRoles eine Liste aller im Container gefundenen Objekte (untergeordnete Objekte) und startet dann nacheinander die Löschung der aufgeführten Objekte.
- Dann führt Quest One ActiveRoles für jedes Objekt in der Liste eine Zugriffskontrolle durch, um zu ermitteln, ob der Benutzer oder Prozess, der die Löschung angefordert hat, über ausreichende Rechte zum Löschen des Objekts verfügt. Wenn die Zugriffskontrolle den Löschvorgang zulässt, dann wird das Objekt gelöscht, andernfalls löscht Quest One ActiveRoles das Objekt nicht und fährt mit der Löschung des nachfolgenden Objektes in der Liste fort.
- Wenn schließlich alle untergeordneten Objekte gelöscht wurden, löscht Quest One ActiveRoles den Container selbst. Wenn alle untergeordneten Objekte gelöscht sind, löscht ActiveRoles Server den Container selbst. Wenn irgendwelche der untergeordneten Objekte nicht gelöscht wurden (zum Beispiel aufgrund von unzureichenden Rechte zum Löschen seitens der anfordernden Instanz), wird der Container ebenfalls nicht gelöscht.

Als Folge dieses Verhaltens kann ein Administrator, der über einen Vollzugriff auf eine Organisationseinheit in Quest One ActiveRoles verfügt, versehentlich die gesamte Organisationseinheit mit all ihren Inhalten in einem einzigen Vorgang löschen. Um dies zu verhindern, bietet Quest One ActiveRoles eine bestimmte Richtlinie, die das Löschen von nicht leeren Containern verhindert.

Die Richtlinie zur Vermeidung einer Containerlöschung definiert eine konfigurierbare Liste der Namen von Objekttypen wie durch das Active Directory-Schema angegeben (zum Beispiel der Objekttyp „Organisationseinheit"). Wenn ein Quest One ActiveRoles-Client die Löschung eines bestimmten Containers anfordert, wertet der Verwaltungsdienst die Anforderung aus, um zu ermitteln, ob sich der Containertyp in der von dieser Richtlinie definierten Liste befindet. Wenn sich der Containertyp in der

Liste befindet und der Container irgendwelche Objekte enthält, verweigert der Verwaltungsdienst die Anforderung und verhindert somit die Löschung des Containers. In diesem Fall fordert der Client den Benutzer auf, alle in dem Container befindlichen Objekte zu löschen, bevor versucht wird, den Container selbst zu löschen.

Gehen Sie folgendermaßen vor, um eine Richtlinie zur Vermeidung einer Containerlöschung zu konfigurieren:

1. Wählen Sie in der Konsolenstruktur **Configuration | Policies | Administration | Builtin.**
2. Doppelklicken Sie im Bereich „Details" auf **Built-in Policy – Container Deletion Prevention**
3. Wählen Sie auf der Registerkarte **Richtlinien** die Richtlinie aus der Liste aus und klicken Sie dann auf **Anzeigen/Bearbeiten**.
4. Gehen Sie auf der Registerkarte **Containertypen** folgendermaßen vor:
   a) Klicken Sie auf **Hinzufügen**.
   b) Wählen Sie im Dialogfeld **Objekttyp wählen** die Containertypen aus, die Sie schützen möchten, und klicken Sie dann auf **OK**.

   So können Sie zum Beispiel den Objekttyp „Organisationseinheit" auswählen, um das Löschen von nicht leeren Organisationseinheiten zu verhindern.
5. Klicken Sie auf **OK**, um die von Ihnen geöffneten Dialogfelder zu schließen.

Das integrierte Richtlinienobjekt, das Sie mit Hilfe der oben aufgeführten Anweisungen konfiguriert haben, verhindert die Löschung von nicht leeren Containern in jeder beliebigen verwalteten Domäne.

Es kann erforderlich sein, dass Quest One ActiveRoles das Löschen von nicht leeren Containern, die sich außerhalb eines bestimmten Bereichs befinden (wie etwa eine bestimmte Domäne, Organisationseinheit oder verwaltete Einheit) nicht verhindern soll, während das Löschen von nicht leeren Containern, die in diesen bestimmten Bereich fallen, verhindert werden soll. In diesem Szenario müssen Sie eine Kopie des integrierten Richtlinienobjekts erstellen und konfigurieren und diese Kopie dann auf den betreffenden Bereich anwenden. Blockieren Sie dann die Auswirkungen des integrierten Richtlinienobjekts, indem Sie das Kontrollkästchen **Alle in diesem Richtlinienobjekt enthaltenen Richtlinien deaktivieren** auf der Registerkarte **Richtlinien** im Dialogfeld für die Verwaltung der Eigenschaften des Richtlinienobjekts aktivieren.

Wenn Sie nur das Löschen von nicht leeren Containern innerhalb eines bestimmten Bereichs zulassen möchten, dann können Sie einfach die Auswirkungen des integrierten Richtlinienobjekts auf das Objekt, das für den betreffenden Bereich steht, blockieren. Wenn Sie also das Löschen von Organisationseinheiten zulassen möchten, die in eine bestimmte verwaltete Einheit fallen, können Sie den Befehl **Richtlinie erzwingen** auf diese verwaltete Einheit anwenden, um das Dialogfeld für die Verwaltung von Richtlinieneinstellungen anzuzeigen und um dann das Kontrollkästchen **Gesperrt** neben dem Namen des integrierten Richtlinienobjekts zu aktivieren.

Objekte vor versehentlichem Löschen schützen

Eine weitere Option, Organisationseinheiten vor versehentlicher Löschung zu schützen, besteht in der Nutzung einer ActiveRoles-Funktion, mit der Sie die Löschung bestimmter Objekte ablehnen können. Bei der Erstellung einer neuen Organisationseinheit mit ActiveRoles haben Sie die Option, die neu erstellte Organisationseinheit vor der Löschung zu schützen. Sie können auch ActiveRoles verwenden, um diesen Schutz für jegliche vorhandene Organisationseinheiten oder andere Objekte in den verwalteten Active Directory-Domänen und Active Directory Lightweight Directory Services (AD LDS) Partitionen zu aktivieren.

Auf den Seiten zur Erstellung einer Organisationseinheit in der ActiveRoles-Konsole oder im Web-Interface können Sie das Kontrollkästchen **Container vor versehentlichem Löschen schützen** aktivieren. Diese Option entfernt die Berechtigungen „Löschen" und „Unterstruktur löschen" für die Organisationseinheit und die Berechtigung „Alle untergeordneten Objekte löschen" für den übergeordneten Container der Organisationseinheit. Eine mit dieser Option erstellte Organisationseinheit kann weder mittels ActiveRoles noch mit anderen Tools für die Active Directory-Verwaltung gelöscht werden, da mit dem Löschvorgang zusammenhängende Berechtigungen durch Anwenden der entsprechenden Zugriffsvorlagen in ActiveRoles und Replizieren der resultierenden Berechtigungseinträge auf Active Directory entfernt werden.

Die Option zum Schützen vorhandener Organisationseinheiten oder anderer Objekte vor versehentlichem Löschen ist auf der Registerkarte **Objekt** der Seite **Eigenschaften** für ein Objekt in der ActiveRoles MMC-Konsole oder im Web-Interface verfügbar. Wenn Sie das Kontrollkästchen **Objekte vor versehentlichem Löschen schützen** auf dieser Registerkarte aktivieren, konfiguriert ActiveRoles die Berechtigungseinträge für das Objekt auf gleiche Weise wie mit der Option **Container vor versehentlichem Löschen schützen** für eine Organisationseinheit. Wenn jemand versucht, ein geschütztes Objekt zu löschen, wird eine Fehlermeldung angezeigt, die angibt, dass das Objekt geschützt oder der Zugriff verweigert wird.

Die Option zum Schützen eines Objekts vor versehentlichem Löschen fügt die folgenden Zugriffsvorlagenverknüpfungen hinzu:

- Fügt für das zu schützende Objekt eine Verknüpfung zur Zugriffsvorlage „Objekte - Löschen verweigern" für die Gruppe „Alle" hinzu.
- Fügt im übergeordneten Container des Objekts eine Verknüpfung zur Zugriffsvorlage „Objekte - Löschen untergeordneter Objekte verweigern" für die Gruppe „Alle" hinzu. (ActiveRoles fügt diese Verknüpfung nicht hinzu, wenn es erkennt, dass bereits eine Verknüpfung derselben Konfiguration vorhanden ist.)

Die Verknüpfungen sind so konfiguriert, dass Sie die Zugriffsvorlagen-Berechtigungseinträge nicht nur in ActiveRoles sondern auch in Active Directory anwenden. Dies fügt die folgenden Zugriffskontrollleinträge (access control entries, ACEs) in Active Directory hinzu:

- Fügt für das zu schützende Objekt explizite Ablehnungs-ACEs für die Berechtigungen „Löschen" und „Unterstruktur löschen" für die Gruppe „Alle" hinzu.
- Fügt im übergeordneten Container des Objekts einen expliziten Ablehnungs-ACE für die Berechtigung „Alle untergeordneten Objekte löschen" für die Gruppe „Alle" hinzu. (ActiveRoles fügt diesen ACE nicht hinzu, wenn es erkennt, dass bereits ein ACE derselben Konfiguration vorhanden ist.)

Wenn Sie das Kontrollkästchen **Objekte vor versehentlichem Löschen schützen** für ein bestimmtes Objekt deaktivieren, aktualisiert ActiveRoles das Objekt, um die Verknüpfung zur Zugriffsvorlage „Objekte - Löschen verweigern" in ActiveRoles gemeinsam mit den expliziten Ablehnungs-ACEs für die Berechtigungen „Löschen" und „Unterstruktur löschen" für die Gruppe „Alle" in Active Directory zu entfernen. Als Folge wird das Objekt nicht weiter gegen versehentliches Löschen geschützt. Beachten Sie, dass die Deaktivierung des Kontrollkästchens für ein bestimmtes Objekt die Zugriffsvorlagenverknüpfungen und ACEs nur von diesem Objekt entfernt und die Zugriffsvorlagenverknüpfungen und ACEs für den übergeordneten Container beibehalten werden. Dies erfolgt, weil der übergeordnete Container andere Objekte enthalten kann, die möglicherweise vor versehentlichem Löschen geschützt sind. Wenn der Container keine geschützten Objekte enthält, können Sie die Verknüpfung zur Zugriffsvorlage „Objekte - Löschen untergeordneter Objekte verweigern" entfernen, indem Sie den Befehl **Kontrolle delegieren** für diesen Container in der ActiveRoles MMC-Konsole anwenden, was auch zum Löschen des entsprechenden ACE in Active Directory führt.

Es ist möglich, ActiveRoles so zu konfigurieren, dass das Kontrollkästchen **Container vor versehentlichem Löschen schützen** standardmäßig auf den Seiten zur Erstellung von Organisationseinheiten in der ActiveRoles-Konsole oder im Web-Interface aktiviert ist. Um dieses Verhalten innerhalb einer Domäne oder eines Containers zu aktivieren, wenden Sie das Richtlinienobjekt „Built-in Policy - Option zum Schützen der OE vor dem Löschen setzen" auf diese Domäne oder diesen Container an. Dieses Richtlinienobjekt gewährleistet, dass von ActiveRoles erstellte Organisationseinheiten unabhängig von der für deren Erstellung verwendeten Methode vor dem Löschen geschützt sind. Folglich werden mittels ActiveRoles Skript-Benutzeroberflächen erstellte Organisationseinheiten ebenfalls standardmäßig geschützt.

Richtlinienerweiterungen

In Quest One ActiveRoles können Administratoren mit Quest One ActiveRoles installierte vordefinierte Richtlinien konfigurieren. Standardmäßig enthält die Liste der Richtlinientypen in der Quest One ActiveRoles-Konsole nur die vordefinierten Typen wie etwa **Automatische Stammordner-Bereitstellung** oder **Benutzerkontodeprovisionierung**. Es ist möglich, die Liste durch Hinzufügen neuer Richtlinientypen zu erweitern.

Jeder Richtlinientyp legt einen bestimmten Richtlinienvorgang (zum Beispiel die Erstellen eines Stammordners für ein Benutzerkonto) zusammen mit einer Reihe von Richtlinienparametern fest, um den Richtlinienvorgang zu konfigurieren (zum Beispiel Parameter, die den Netzwerkspeicherort angeben, an dem die Stammordner erstellt werden sollen). Quest One ActiveRoles ermöglicht die Implementierung und Bereitstellung von benutzerdefinierten Richtlinientypen. ActiveRoles Server ermöglicht die Erstellung von benutzerdefinierten Richtlinientypen sowie die Auflistung zusammen mit den vordefinierten Richtlinientypen, was den Administratoren ermöglicht, Richtlinien zu konfigurieren, die von diesen neuen Richtlinientypen festgelegte benutzerdefinierte Vorgänge durchführen.

Quest One ActiveRoles ermöglicht die Erstellung von benutzerdefinierten Richtlinien, die auf dem integrierten Richtlinientyp „Skriptausführung" basieren. Die Erstellung und Konfiguration einer Skriptrichtlinie von Grund auf kann jedoch zeitaufwändig sein. Benutzerdefinierte Richtlinientypen bieten eine Möglichkeit, dieses zeitaufwendige Verfahren abzukürzen. Sobald ein benutzerdefinierter Richtlinientyp bereitgestellt ist, der auf ein bestimmtes Skript verweist, können Administratoren auf einfache Weise Richtlinien dieses Typs konfigurieren und anwenden, sodass diese Richtlinien die von diesem Skript vorgegebenen Vorgänge ausführen. Das Richtlinienskript definiert auch die für den Richtlinientyp spezifischen Richtlinienparameter.

Benutzerdefinierte Richtlinientypen bieten einen erweiterbaren Mechanismus für die Bereitstellung von benutzerdefinierten Richtlinien. Diese Möglichkeit wird über die Objektklasse „Richtlinientyp" implementiert. Richtlinientyp-Objekte können mit Hilfe der Quest One ActiveRoles-Konsole erstellt werden, wobei jedes Objekt einen bestimmten benutzerdefinierten Richtlinientyp angibt.

Designelemente

Die Richtlinien-Erweiterungsfunktion stützt sich auf zwei Interaktionen: Richtlinientyp-Bereitstellung und Richtlinientyp-Nutzung.

Richtlinientyp-Bereitstellung

Das Bereitstellungsverfahren umfasst die Entwicklung eines Skripts, das die Richtlinienaktion implementiert und die Richtlinienparameter deklariert; die Erstellung eines Skriptmoduls, das das Skript enthält; und die Erstellung eines Richtlinientypobjekts, das sich auf dieses Skriptmodul bezieht. Um einen Richtlinientyp in einer anderen Umgebung bereitzustellen, kann ein Administrator den Richtlinientyp in eine Exportdatei in der Quellumgebung exportieren und die Datei dann in die Zielumgebung importieren. Die Verwendung von Exportdateien erleichtert die Verbreitung von benutzerdefinierten Richtlinientypen.

Richtlinientyp-Nutzung

Die Richtlinientyp-Nutzung ist der Prozess der Konfiguration von Richtlinien. Dieser Prozess läuft ab, wenn ein Administrator ein neues Richtlinienobjekt erstellt oder Richtlinien zu einem vorhandenen Richtlinienobjekt hinzufügt. Der Assistent für die Erstellung eines Richtlinienobjekts umfasst zum Beispiel eine Seite, die zur Auswahl einer Richtlinie auffordert. Auf der Seite werden die in Quest One ActiveRoles definierten Richtlinientypen einschließlich der benutzerdefinierten Richtlinientypen aufgelistet. Wenn ein benutzerdefinierter Richtlinien

typ ausgewählt wird, bietet der Assistent eine Seite für die Konfiguration der für diesen Richtlinien typ spezifischen Richtlinienparameter an. Nach Fertigstellung des Assistenten enthält das Richtlinienobjekt eine voll funktionsfähige Richtlinie des ausgewählten benutzerdefinierten Typs.

Quest One ActiveRoles bietet eine grafische Benutzeroberfläche einschließlich einer programmierbaren Schnittstelle für die Erstellung und Verwaltung von benutzerdefinierten Richtlinientypen. Mit Hilfe dieser Schnittstellen können Quest One ActiveRoles-Richtlinien erweitert werden, um den Anforderungen einer bestimmten Umgebung zu entsprechen. Quest One ActiveRoles verfügt weiterhin über einen Bereitstellungsmechanismus, mit dem Administratoren neue Richtlinientypen in Betrieb nehmen können.

Da die Richtlinienerweiterung zwei Interaktionen umfasst, bietet Quest One ActiveRoles Lösungen auf beiden Gebieten. Der Verwaltungsdienst behält die Richtlinientypdefinitionen bei und stellt die Richtlinientypen seinen Clients wie etwa der Quest One ActiveRoles-Konsole oder ADSI Provider bereit. Die Konsole kann für folgende Vorgänge verwendet werden:

- Erstellen eines neuen benutzerdefinierten Richtlinientyps, entweder von Grund auf oder per Import eines Richtlinientyps, der aus einer anderen Umgebung exportiert wurde.
- Vornehmen von Änderungen an der Definition eines vorhandenen benutzerdefinierten Richtlinientyps.
- Hinzufügen einer Richtlinie eines bestimmten benutzerdefinierten Typs zu einem Richtlinienobjekt, wodurch die erforderlichen Änderungen an den von der Richtlinientypdefinition bereitgestellten Richtlinienparametern vorgenommen werden.

Normalerweise entwickelt ein Quest One ActiveRoles-Experte einen benutzerdefinierten Richtlinientyp in einer separaten Umgebung und exportiert dann den Richtlinientyp in eine Exportdatei. Ein Quest One ActiveRoles-Administrator stellt dann den Richtlinientyp durch Import der Exportdatei in der Produktionsumgebung bereit. Anschließend kann die Quest One ActiveRoles-Konsole für die Konfiguration und Anwendung der Richtlinien dieses neuen Typs verwendet werden.

Richtlinientypobjekte

Die Richtlinienerweiterbarkeit beruht auf Richtlinientypobjekten, von denen jedes einen einzigen Richtlinientyp angibt. Richtlinientypobjekte werden sowohl bei der Richtlinientyp-Bereitstellung als auch bei der Richtlinientyp-Nutzung verwendet. Der Prozess der Bereitstellung eines neuen Richtlinientyps umfass die Erstellung eines Richtlinientypobjekts. Während des Hinzufügens einer benutzerdefinierten Richtlinie wird die Richtlinientypdefinition vom entsprechenden Richtlinientypobjekt abgerufen.

Jedes Richtlinientypobjekt enthält die folgenden Daten für die Definition eines einzelnen Richtlinientyps:

- **Anzeigename.** Gibt den von diesem Richtlinientypobjekt dargestellten Richtlinientyp an. Dieser Name wird auf der Assistentenseite angezeigt, auf der Sie eine zu konfigurierende Richtlinie auswählen, wenn Sie ein neues Richtlinienobjekt erstellen oder eine Richtlinie zu einem vorhandenen Richtlinienobjekt hinzufügen.
- **Beschreibung.** Ein Text, der den Richtlinientyp beschreibt. Dieser Text wird angezeigt, wenn Sie den Richtlinientyp im Assistenten zur Erstellung eines neuen Richtlinienobjekts oder im Assistenten zum Hinzufügen einer Richtlinie zu einem vorhandenen Richtlinienobjekt auswählen.
- **Verweis auf ein Skriptmodul.** Gibt das Skript an, das bei der Ausführung einer Richtlinie dieses Typs ausgeführt werden soll. Wenn Sie eine Richtlinie eines benutzerdefinierten Richtlinientyps hinzufügen, erstellen Sie effektiv eine Richtlinie, die das Skript aus dem Skriptmodul ausführt, das vom entsprechenden Richtlinientypobjekt angegeben wird.

- **Richtlinientypkategorie.** Gibt die Kategorie des Richtlinienobjekts an, zu dem eine Richtlinie dieses Typs hinzugefügt werden kann. Für einen Richtlinientyp kann die Kategorieoption entweder auf „Bereitstellung" oder „Deprovisionierung" gesetzt sein, was das Hinzufügen von Richtlinien dieses Typs zu Bereitstellungs- bzw. Deprovisionsrichtlinienobjekten ermöglicht.
- **Funktion zur Deklaration von Parametern.** Gibt den Namen der Skriptfunktion an, die die konfigurierbaren Parameter für die Verwaltungsrichtlinie deklariert, die auf diesem Richtlinientyp basiert. Die Funktion muss in dem für den Richtlinientyp ausgewählten Skriptmodul vorhanden sein. Standardmäßig wird vorausgesetzt, dass die Parameter von der Funktion mit der Bezeichnung „onInit" deklariert werden.
- **Richtlinientypsymbol.** Das Bild, das neben dem Anzeigenamen des Richtlinientyps auf der Assistentenseite angezeigt wird, auf der Sie eine zu konfigurierende Richtlinie auswählen, um die Identifizierung und visuelle Unterscheidung dieses Richtlinientyps von anderen Richtlinientypen zu erleichtern.

Um einen benutzerdefinierten Richtlinientyp zu erstellen, müssen Sie zunächst ein Skriptmodul erstellen, das das Richtlinienskript enthält. Dann können Sie ein Richtlinientypobjekt erstellen, das auf dieses Skriptmodul verweist. Wenn Sie einen Richtlinientyp importieren, erstellt Quest One ActiveRoles automatisch sowohl das Skriptmodul als auch das Richtlinientypobjekt für diesen Richtlinientyp. Nach der Erstellung des Richtlinientypobjekts können Sie eine Richtlinie dieses neuen Typs zu einem Richtlinienobjekt hinzufügen.

Erstellen und Verwalten von benutzerdefinierten Richtlinientypen

In Quest One ActiveRoles bieten Richtlinientypobjekte die Möglichkeit, die Definition eines benutzerdefinierten Richtlinientyps in einem einzelnen Objekt zu speichern. Richtlinientypobjekte können exportiert und importiert werden. Dies erleichtert die Verbreitung von benutzerdefinierten Richtlinien in anderen Umgebungen.

Wenn Sie ein neues Richtlinienobjekt erstellen oder eine Richtlinie zu einem vorhandenen Richtlinienobjekt hinzufügen, wird einem Administrator eine Liste der von den Richtlinientypobjekten abgeleiteten Richtlinientypen angezeigt. Bei Auswahl eines benutzerdefinierten Richtlinientyps aus der Liste erstellt Quest One ActiveRoles eine Richtlinie auf der Grundlage der im entsprechenden Richtlinientypobjekt gefundenen Einstellungen.

Dieser Abschnitt deckt die folgenden, für benutzerdefinierte Richtlinientypen spezifischen Aufgaben ab:

- Erstellen eines Richtlinientypobjekts
- Ändern eines vorhandenen Richtlinientypobjekts
- Verwenden von Richtlinientypcontainern
- Exportieren von Richtlinientypen
- Importieren von Richtlinientypen
- Konfigurieren einer Richtlinie eines benutzerdefinierten Typs
- Löschen eines Richtlinientypobjekts

Weitere Informationen über Richtlinientypobjekte und Anweisungen bezüglich der Skripterstellung für Richtlinientypobjekte finden Sie in der Dokumentation zum Quest One ActiveRoles SDK.

Erstellen eines Richtlinientypobjekts

Quest One ActiveRoles speichert Richtlinientypobjekte im Container **Policy Types**. Sie können auf diesen Container in der Quest One ActiveRoles-Konsole zugreifen, indem Sie den Zweig **Configuration/Server Configuration** der Konsolenstruktur erweitern.

Gehen Sie folgendermaßen vor, um ein neues Richtlinientypobjekt zu erstellen:

1. Klicken Sie in der Konsolenstruktur unter **Configuration/Server** Configuration/Policy Types mit der rechten Maustaste auf den Richtlinientypcontainer, in dem Sie ein neues Objekt erstellen möchten, und wählen Sie dann **Neu | Richtlinientyp**.

   *Wenn Sie zum Beispiel ein neues Objekt im Root-Container erstellen möchten, klicken Sie mit der rechten Maustaste auf **Richtlinientypen**.*

2. Geben Sie im Assistenten „Neues Objekt - Richtlinientyp" einen Namen, einen Anzeigenamen und optional eine Beschreibung für das neue Objekt ein.

   Der Anzeigename und die Beschreibung werden auf der Seite zur Auswahl einer Richtlinie in den Assistenten, die für die Konfiguration von Richtlinienobjekten verwendet werden, angezeigt.

3. Klicken Sie auf **Weiter**.
4. Klicken Sie auf **Durchsuchen** und wählen Sie das Skriptmodul, das das Skript enthält, das von den Richtlinien dieses Richtlinientyps ausgeführt wird.

   Das Skriptmodul muss im Container „Configuration/Script Modules" vorhanden sein und ein Richtlinienskript enthalten. Weitere Informationen über Richtlinienskripts finden Sie in der Quest One ActiveRoles SDK-Dokumentation.

5. Gehen Sie im Bereich **Richtlinientypkategorie** wie nachfolgend beschrieben vor:
   - Klicken Sie auf **Bereitstellung**, wenn Richtlinien dieses Typs für Richtlinienobjekte der Kategorie „Bereitstellung" vorgesehen sind.
   - Klicken Sie auf **Deprovisionierung**, wenn Richtlinien dieses Typs für Richtlinienobjekte der Kategorie „Deprovisionierung" vorgesehen sind.

   *Die Richtlinientypen, für die die Option **Bereitstellung** ausgewählt ist, werden auf der Seite zur Auswahl einer Richtlinie in dem Assistenten angezeigt, der für die Erstellung eines Bereitstellungsrichtlinienobjekts oder zum Hinzufügen von Richtlinien zu einem vorhandenen Bereitstellungsrichtlinienobjekt verwendet wird. Umgekehrt werden die Richtlinientypen, für die die Option **Deprovisionierung** ausgewählt ist, in dem Assistenten zur Erstellung eines Deprovisionsrichtlinienobjekts oder zum Hinzufügen von Richtlinien zu einem solchen Richtlinienobjekt angezeigt.*

6. Wählen Sie aus der Liste **Funktion zur Deklaration von Parametern** den Namen der Skriptfunktion, die die Parameter definiert, die für diesen Verwaltungsrichtlinientyp spezifisch sind.

   *Die Liste enthält die Namen aller Funktionen, die in dem von Ihnen in Schritt 4 ausgewählten Skript gefunden wurden. Jede Richtlinie dieses Typs verfügt über die Parameter, die durch die **Funktion angegeben werden, die Sie aus der Liste Funktion zur Deklaration von Parametern** auswählen. Normalerweise ist dies eine Funktion mit der Bezeichnung „onInit" (ausführlichere Informationen finden Sie im Quest One ActiveRoles Software Development Kit (SDK)).*

7. Klicken Sie auf **Richtlinientyp-Symbol**, um das Bild anzuzeigen, das diesen Richtlinientyp angibt. Um ein anderes Bild auszuwählen, klicken Sie auf **Ändern** und öffnen dann eine Symboldatei, die das gewünschte Bild enthält.

   Dieses Bild wird neben dem Anzeigenamen des Richtlinientyps auf der Assistentenseite zur Auswahl einer zu konfigurierenden Richtlinie angezeigt, um die Identifizierung und visuelle Unterscheidung dieses Richtlinientyps von anderen Richtlinientypen zu erleichtern.

*Das Bild wird im Richtlinientypobjekt gespeichert. In dem Dialogfeld, das durch Anklicken von **Richtlinientyp-Symbol** angezeigt wird, können Sie das aktuell verwendete Bild sehen. Um wieder das Standardbild zu verwenden, klicken Sie auf **Standardsymbol verwenden**. Wenn die Schaltfläche nicht verfügbar ist, dann wird aktuell das Standardbild verwendet.*

8. Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um die Erstellung des neuen Richtlinientypobjekts abzuschließen.

Ändern eines vorhandenen Richtlinientypobjekts

Sie können ein vorhandenes Richtlinientypobjekt ändern, indem Sie die allgemeinen Eigenschaften, das Skript, die Kategorie oder das Symbol ändern. Die allgemeinen Eigenschaften umfassen den Namen, den Anzeigenamen und die Beschreibung. Die Richtlinientypobjekte befinden sich unter **Configuration/ Server Configuration/Policy Types** in der Quest One ActiveRoles-Konsole.

Die folgende Tabelle fasst die Änderungen zusammen, die Sie an einem vorhandenen Richtlinientypobjekt vornehmen können, vorausgesetzt, dass Sie das Objekt in der Quest One ActiveRoles-Konsole gefunden haben.

ÄNDERUNG VON	VORGEHENSWEISE	KOMMENTAR
Name des Objekts	Klicken Sie mit der rechten Maustaste auf das Objekt und klicken Sie dann auf **Umbenennen**.	Der Name wird verwendet, um das Objekt zu identifizieren, und muss für die im selben Richtlinientypcontainer enthaltenen Objekte eindeutig sein.
Anzeigename oder Beschreibung	Klicken Sie mit der rechten Maustaste auf das Objekt, klicken Sie auf **Eigenschaften** und nehmen Sie die erforderlichen Änderungen auf der Registerkarte **Allgemein** vor.	Durch die Änderung des Anzeigenamens oder der Beschreibung ändert sich auch der Richtlinienname bzw. die Richtlinienbeschreibung auf der Seite zur Auswahl einer Richtlinie in den Assistenten zur Verwaltung von Richtlinienobjekten.
Skriptmodul	Klicken Sie mit der rechten Maustaste auf das Objekt, klicken Sie auf **Eigenschaften**, dann auf die Registerkarte **Skript**, anschließend auf **Durchsuchen** und wählen Sie dann das gewünschte Skriptmodul aus.	Sie können das Skript in dem Skriptmodul ändern, das aktuell mit dem Richtlinientypobjekt verbunden ist, anstatt ein anderes Skriptmodul auszuwählen. Um das Skript anzuzeigen oder zu ändern, suchen Sie das Skript Modul in der Quest One ActiveRoles-Konsolenstruktur unter **Configuration/Script Modules** und wählen es aus. Die Änderung des Skripts beeinflusst alle vorhandenen Richtlinien dieses Richtlinientyps. Wenn Sie eine Richtlinie zu einem Richtlinienobjekt hinzufügen und dann das Skript für das Richtlinientypobjekt ändern, auf dessen Grundlage die Richtlinie erstellt wurde, dann führt die Richtlinie das geänderte Skript aus.

ÄNDERUNG VON	VORGEHENSWEISE	KOMMENTAR
Kategorie des Richtlinientyps	Klicken Sie mit der rechten Maustaste auf das Objekt, klicken Sie auf **Eigenschaften**, dann auf die Registerkarte **Skript** und anschließend entweder auf **Bereitstellung** oder auf **Deprovisionierung**.	Durch die Änderung dieser Option ändert sich auch die Darstellung des entsprechenden Richtlinientyps in den Assistenten zur Verwaltung von Richtlinienobjekten. Wenn zum Beispiel die Option von **Bereitstellung** in **Deprovisionierung** geändert wird, wird der Richtlinientyp nicht mehr im Assistenten zur Konfiguration eines Bereitstellungsrichtlinienobjekts angezeigt; statt dessen wird er im Assistenten zur Konfiguration eines Deprovisionsrichtlinienobjekts angezeigt. Die Änderung der Richtlinientypkategorie hat jedoch keinen Einfluss auf die vorhandenen Richtlinien dieses Richtlinientyps. Wenn zum Beispiel eine Richtlinie zu einem Bereitstellungsrichtlinienobjekt hinzugefügt wird, dann bleibt die Richtlinie in diesem Richtlinienobjekt erhalten, selbst wenn die Richtlinientypkategorie von **Bereitstellung** in **Deprovisionierung** im entsprechenden Richtlinientypobjekt geändert wird.
Funktion zur Deklaration von Parametern	Klicken Sie mit der rechten Maustaste auf das Objekt, klicken Sie dann auf **Eigenschaften**, anschließend auf die Registerkarte **Skript**und wählen Sie dann die entsprechende Funktion aus der Liste **Funktion zur Deklaration von Parametern** aus.	Die Änderung dieser Einstellung ändert die Liste der für diesen Richtlinientyp spezifischen Richtlinienparameter. Die Änderungen haben keinen Einfluss auf die Parameter der vorhandenen Richtlinien dieses Typs. Wenn Sie eine neue, auf diesem Richtlinientyp basierende Richtlinie hinzufügen, wird die Liste der Richtlinienparameter mit Hilfe der neuen Funktion zur Deklaration von Parametern erstellt.
Richtlinientyp-Symbol	Klicken Sie mit der rechten Maustaste auf das Objekt, klicken Sie auf **Eigenschaften** und dann auf die Registerkarte **Skript**, klicken Sie anschließend auf **Richtlinientyp-Symbol** und gehen Sie dann wie nachfolgend beschrieben vor: • Klicken Sie auf **Ändern** und öffnen Sie eine Symboldatei, die das gewünschte Symbol enthält. • Klicken Sie auf **Standardsymbol verwenden**, um wieder das Standardbild zu verwenden.	Durch die Änderung dieser Einstellung ändert sich auch das Bild, das neben dem Anzeigenamen des Richtlinientyps in den Assistenten zur Verwaltung von Richtlinienobjekten auf der Seite angezeigt wird, auf der Sie zur Auswahl einer zu konfigurierenden Richtlinie aufgefordert werden.

Verwenden von Richtlinientypcontainern

Sie können einen Richtlinientypcontainer für die Speicherung zugehöriger Richtlinientypobjekte und anderer Richtlinientypcontainer verwenden.

Container bieten die Möglichkeit einer zusätzlichen Kategorisierung von benutzerdefinierten Richtlinientypen und erleichtern somit das Auffinden und die Auswahl der zu konfigurierenden Richtlinie in den Assistenten zur Verwaltung von Richtlinienobjekten. Wenn Sie also ein Richtlinienobjekt erstellen, werden auf der Assistentenseite, auf der Sie zur Auswahl einer Richtlinie aufgefordert werden, die benutzerdefinierten Richtlinientypen zusammen mit den Containern, in denen sich die entsprechenden Richtlinientypobjekte befinden, angezeigt.

Gehen Sie folgendermaßen vor, um einen neuen Richtlinientypcontainer zu erstellen:

1. Klicken Sie in der Konsolenstruktur unter **Configuration/Server Configuration/Policy Types** mit der rechten Maustaste auf den Richtlinientypcontainer, in dem Sie einen neuen Container erstellen möchten, und wählen Sie dann **Neu | Richtlinientypcontainer**.

   *Wenn Sie zum Beispiel einen neuen Container im Root-Container erstellen möchten, klicken Sie mit der rechten Maustaste auf **Richtlinientypen**.*

2. Geben Sie im Assistenten „Neues Objekt – Richtlinientypcontainer" einen Namen und optional eine Beschreibung für den neuen Container ein.

   Der Name und die Beschreibung werden auf der Seite zur Auswahl einer Richtlinie in den Assistenten, die für die Konfiguration von Richtlinienobjekten verwendet werden, angezeigt.

3. Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um die Erstellung des neuen Containers abzuschließen.

Exportieren von Richtlinientypen

Sie können Richtlinientypobjekte exportieren, sodass die Definition der Richtlinientypen in einer XML-Datei gespeichert wird, die in eine andere Quest One ActiveRoles-Umgebung importiert werden kann. Das Exportieren und anschließende Importieren von Richtlinientypobjekten erleichtert die Verbreitung von benutzerdefinierten Richtlinien in anderen Umgebungen.

Gehen Sie folgendermaßen vor, um ein Richtlinientypobjekt oder einen Container zu exportieren:

- Klicken Sie mit der rechten Maustaste auf das Richtlinientypobjekt oder den Container in der Quest One ActiveRoles-Konsole, klicken Sie dann auf **Exportieren** und geben Sie eine XML-Datei für die Speicherung der Exportdaten an.

Sie können mehrere zu exportierende Richtlinienobjekte auswählen oder Sie können einen Container auswählen, um alle in diesem Container befindlichen Richtlinientypobjekte und Container zu exportieren. In beiden Fällen erstellt der Exportvorgang eine einzelne XML-Datei, die später in jeden beliebigen Container unter dem Knoten **Policy Types** importiert werden kann.

Beim Export von Richtlinientypobjekten wird eine XML-Datei erstellt, die sowohl die Objekte als auch die Skriptmodule angibt, die die Richtlinienskripts für jeden zu exportierenden Richtlinientyp angibt. Während eines Imports erstellt Quest One ActiveRoles Richtlinientypobjekte und die Skriptmodule auf der Grundlage der Daten in der XML-Datei. Als Ergebnis des Imports werden Richtlinientypen in der neuen Umgebung repliziert; diese können dann auf gleiche Weise wie in der Umgebung, aus der sie exportiert wurden, verwendet werden.

Importieren von Richtlinientypen

Sie können die exportierten Richtlinientypobjekte und Container importieren. Hierdurch werden sie zum Richtlinientypcontainer hinzugefügt, was Ihnen ermöglicht, von diesen Richtlinientypobjekten festgelegte Richtlinien zu konfigurieren und zu verwenden. Alle für die Bereitstellung der Richtlinientypen erforderlichen Daten sind in einer XML-Datei enthalten. Um ein Beispiel für das XML-Dokument anzuzeigen, das einen Richtlinientyp angibt, exportieren Sie ein Richtlinientypobjekt und betrachten dann die gespeicherte XML-Datei.

Gehen Sie folgendermaßen vor, um die exportierten Richtlinientypobjekte und Container zu importieren:

1. Klicken Sie in der Quest One ActiveRoles-Konsolenstruktur unter **Configuration/Server Configuration/Policy Types** mit der rechten Maustaste auf den Richtlinientypcontainer, in den Sie die exportierten Richtlinientypobjekte und Container importieren möchten.
2. Klicken Sie auf **Richtlinientypen importieren** und öffnen Sie dann die XML-Datei, die Sie importieren möchten.

Hierdurch werden neue Richtlinientypobjekte und Container im ausgewählten Container erstellt. Außerdem werden neue Skriptmodule im Container **Configuration/Script Modules** erstellt und mit den neu erstellten Richtlinientypobjekten verknüpft.

Konfigurieren einer Richtlinie eines benutzerdefinierten Typs

Wenn ein benutzerdefinierter Richtlinientyp bereitgestellt wurde, kann ein Quest One ActiveRoles-Administrator eine Richtlinie dieses Typs zu einem Richtlinienobjekt hinzufügen. Dies erfolgt durch Auswahl des Richtlinientyps im Assistenten zur Erstellung eines neuen Richtlinienobjekts oder im Assistenten zum Hinzufügen einer Richtlinie zu einem vorhandenen Richtlinienobjekt.

Welcher Assistent zu verwenden ist, hängt von der Kategorie des Richtlinientyps ab:

- Für einen Richtlinientyp der Kategorie „Bereitstellung" kann eine Richtlinie dieses Typs nur zu einem Bereitstellungsrichtlinienobjekt hinzugefügt werden.
- Für einen Richtlinientyp der Kategorie „Deprovisionierung" kann eine Richtlinie dieses Typs nur zu einem Deprovisionsrichtlinienobjekt hinzugefügt werden.

Gehen Sie folgendermaßen vor, um eine Richtlinie eines benutzerdefinierten Richtlinientyps zu konfigurieren:

1. Befolgen Sie die Anweisungen im Assistenten zur Erstellung eines neuen Richtlinienobjekts oder im Assistenten zum Hinzufügen einer Richtlinie zu einem vorhandenen Richtlinienobjekt.

   *Wenn der Richtlinientyp zum Beispiel aus der Kategorie „Bereitstellung" stammt, können Sie den Assistenten zur Erstellung eines neuen Bereitstellungsrichtlinienobjekts verwenden, der durch Anwendung des Befehls **Neu | Bereitstellungsrichtlinie** auf einen Container unter **Configuration/Policies/Administration** in der Quest One ActiveRoles-Konsole geöffnet wird.*

2. Klicken Sie auf der Seite **Zu konfigurierende Richtlinie** im Assistenten auf den gewünschten Richtlinientyp.

   *Auf der Seite **Zu konfigurierende Richtlinie** werden die benutzerdefinierten Richtlinientypen zusammen mit den vordefinierten Quest One ActiveRoles-Richtlinientypen aufgelistet. Jeder benutzerdefinierte Richtlinientyp wird durch den Anzeigenamen des entsprechenden Richtlinientypobjekts identifiziert.*

Die benutzerdefinierten Richtlinientypen sind in einer baumähnlichen Struktur zusammengefasst, die die vorhandene Hierarchie der Richtlinientypcontainer widerspiegelt. Wenn zum Beispiel ein Richtlinientypcontainer erstellt wird, um ein bestimmtes Richtlinientypobjekt zu speichern, wird der Container auch auf der Assistentenseite angezeigt, sodass Sie den Container erweitern müssen, um den Richtlinientyp anzuzeigen oder auszuwählen.

3. Legen Sie auf der Seite **Richtlinienparameter** Parameterwerte für die Richtlinie fest: Klicken Sie auf den Namen eines Parameters in der Liste und klicken Sie dann auf **Bearbeiten**.

   Parameter kontrollieren das Verhalten der Richtlinie. Wenn Quest One ActiveRoles die Richtlinie ausführt, gibt es die Parameterwerte an das Richtlinienskript weiter. Die vom Skript durchgeführten Vorgänge und die Ergebnisse dieser Vorgänge hängen von den Parameterwerten ab.

   *Durch Anklicken von **Bearbeiten** wird eine Seite angezeigt, auf der Sie einen oder mehrere Werte für den ausgewählten Parameter hinzufügen, entfernen oder auswählen können. Für jeden Parameter definiert das Richtlinienskript den Namen des Parameters und andere Merkmale wie etwa eine Beschreibung, eine Liste der akzeptablen Werte, den Standardwert und ob ein Wert erforderlich ist. Wenn eine Liste der akzeptablen Werte definiert ist, dann können Sie nur Werte aus dieser Liste auswählen.*

4. Folgen Sie den Anweisungen des Assistenten, um den Assistenten abzuschließen.

Löschen eines Richtlinientypobjekts

Sie können ein Richtlinientypobjekt löschen, wenn Sie keine Richtlinien des von diesem Objekt angegebenen Typs mehr hinzufügen müssen.

Beachten Sie vor dem Löschen eines Richtlinientypobjekts die folgenden Hinweise:

- Sie können ein Richtlinientypobjekt nur dann löschen, wenn keine Richtlinien des entsprechenden Richtlinientyps in irgendeinem Richtlinienobjekt vorhanden sind. Prüfen Sie jedes Richtlinienobjekt und entfernen Sie die Richtlinien dieses Typs (falls vorhanden) aus dem Richtlinienobjekt, bevor Sie das Richtlinientypobjekt löschen.
- Durch das Löschen eines Richtlinientypobjekts wird dieses dauerhaft aus der Quest One ActiveRoles-Datenbank gelöscht. Wenn Sie diesen Richtlinientyp erneut verwenden möchten, sollten Sie das Richtlinientypobjekt in eine XML-Datei exportieren, bevor Sie das Objekt löschen.
- Durch das Löschen eines Richtlinientypobjekts wird das mit diesem Objekt verbundene Skriptmodul nicht gelöscht. Das Skriptmodul wird nicht gelöscht, da es möglicherweise von anderen Richtlinien verwendet wird. Wenn das Skriptmodul nicht mehr benötigt wird, kann es separat gelöscht werden.

Gehen Sie folgendermaßen vor, um ein Richtlinientypobjekt zu löschen:

- Klicken Sie mit der rechten Maustaste auf das Richtlinientypobjekt in der Quest One ActiveRoles-Konsole und klicken Sie dann auf **Löschen**.

6

Arbeitsabläufe

- Beschreibung des Arbeitsablaufs
- Übersicht über die Arbeitsablaufaktivitäten
- Konfigurieren eines Arbeitsablaufs
- Beispiel: Genehmigungs-Arbeitsablauf
- E-Mail-basierte Genehmigung
- Automatisierungs-Arbeitsablauf
- Aktivitätserweiterungen

Beschreibung des Arbeitsablaufs

Quest One ActiveRoles bietet ein umfassendes Arbeitsablaufsystem für die Automatisierung und Integration der Verwaltung von Verzeichnisdaten. Dieses auf der Windows Workflows Foundation-Technologie von Microsoft basierende Arbeitsablaufsystem ermöglicht IT-Spezialisten, Verwaltungsregeln schnell und einfach zu definieren, zu automatisieren und zu erzwingen. Arbeitsabläufe erweitern die Möglichkeiten von Quest One ActiveRoles, indem sie einen Rahmen bieten, der die Kombination vielseitiger Verwaltungsregeln wie etwa die Bereitstellung und Deprovisionierung von Identitätsinformationen im Verzeichnis, die Durchsetzung von Richtlinienregeln für Änderungen an den Identitätsdaten, die Weiterleitung von Datenänderungen zu Genehmigungszwecken, E-Mail-Benachrichtigungen über bestimmte Ereignisse und Bedingungen sowie die Möglichkeit zur Implementierung benutzerdefinierter Vorgänge mit Hilfe von Skripttechnologien wie etwa Microsoft Windows PowerShell oder VBScript ermöglicht.

Angenommen, Sie müssen Benutzerkonten auf der Grundlage von Daten aus externen Systemen bereitstellen. Die Daten werden abgerufen und dann mit Hilfe eines Dienstes wie etwa ActiveRoles Quick Connect, das in Verbindung mit Quest One ActiveRoles arbeitet, an das Verzeichnis weitergeleitet. Für die Koordination der im Zusammenhang mit der Kontobereitstellung stehenden Vorgänge kann ein Arbeitsablauf erstellt werden. So können zum Beispiel verschiedene Regeln für die Erstellung oder Aktualisierung der in verschiedenen Containern befindlichen Konten angewandt werden.

Arbeitsabläufe können auch Genehmigungsregeln enthalten, die erfordern, dass bestimmte Änderungen von zuvor bestimmten Personen (genehmigende Instanzen) autorisiert werden. Beim Entwurf eines Genehmigungs-Arbeitsablaufs gibt der Administrator an, welche Art von Vorgang zum Start des Arbeitsablaufs führt, und fügt Genehmigungsregeln zum Arbeitsablauf hinzu. Die Genehmigungsregeln legen fest, wer autorisiert ist, den Vorgang zu genehmigen. Sie legen außerdem die erforderliche Reihenfolge der Genehmigungen und die Personen, die über Genehmigungsaufgaben oder Entscheidung informiert werden sollen, fest.

Durch das Senden von E-Mail-Benachrichtigungen erweitern Arbeitsabläufe die Reichweite der Verwaltungprozessautomatisierung auf das gesamte Unternehmen. Benachrichtigungsaktivitäten in einem Arbeitsablauf ermöglichen, Personen per E-Mail über Ereignisse, Bedingungen oder Aufgaben, die ihre Aufmerksamkeit erfordern, zu informieren. So können zum Beispiel Genehmigungsregeln über Änderungsanforderungen informieren, die auf eine Genehmigung warten. Es können auch separate Benachrichtigungsregeln angewandt werden, um über Datenänderungen im Verzeichnis zu informieren. Benachrichtigungsmeldungen umfassen alle erforderlichen unterstützenden Informationen und bieten Hyperlinks, die es den Nachrichtenempfängern ermöglichen, Aktionen mittels eines standardmäßigen Webbrowsers zu ergreifen.

Wichtige Funktionsmerkmale und Definitionen

In diesem Abschnitt sind einige wichtige Konzepte zusammengefasst, die für den Entwurf und die Implementierung von Arbeitsabläufen in Quest One ActiveRoles gelten.

Workflow

Ein Arbeitsablauf ist ein Modell, das einen Prozess beschreibt, der aus Schritten oder Aktivitäten besteht. Arbeitsabläufe beschreiben die Reihenfolge der Ausführung und Beziehungen zwischen Aktivitäten, die für die Durchführung bestimmter Vorgänge erforderlich sind. In Quest One ActiveRoles stellen Arbeitsabläufe eine Möglichkeit dar, Bereitstellungsvorgänge und die allgemeine Verwaltung von Verzeichnisdaten anzupassen. Arbeitsabläufe können also verwendet werden, um Genehmigungen zu Benutzerbereitstellungsprozessen hinzuzufügen oder die Benutzerbereitstellungsprozesse in externe Systeme zu integrieren.

Arbeitsablaufdefinition

Eine Arbeitsablaufdefinition ist eine Darstellung der Arbeitsablaufstruktur. Die Definition eines Arbeitsablaufs wird als ein einzelnes Objekt im Quest One ActiveRoles-Konfigurationsdatenspeicher gespeichert und kann als ein XML-Dokument strukturiert sein, dass die Arbeitsablauf-Startbedingungen, die Aktivitäten, die Parameter für die Aktivitäten und die Reihenfolge, in der die Aktivitäten ausgeführt werden sollen, definiert.

Arbeitsablauf-Startbedingungen

Die Arbeitsablaufeinstellungen, die festlegen, welche Vorgänge zum Start des Arbeitsablaufs führen, werden als „Arbeitsablauf-Startbedingungen" bezeichnet. Ein Arbeitsablauf kann zum Beispiel so konfiguriert sein, dass jede Anforderung zur Erstellung eines Benutzerkontos in einem bestimmten Container den Arbeitsablauf startet.

Arbeitsablaufinstanz

Durch den Start eines Arbeitsablaufs wird eine Arbeitsablaufinstanz auf der Grundlage der Einstellungen in der Arbeitsablaufdefinition erstellt. Jede Arbeitsablaufinstanz speichert die Laufzeitdaten, die den aktuellen Status eines einzelnen, gerade ausgeführten Arbeitsablaufs angeben.

Arbeitsablaufaktivität

Eine Arbeitsablaufaktivität ist eine logisch isolierte Einheit, die einen bestimmten operationalen Schritt eines Arbeitsablaufs implementiert. Die in einer Aktivität enthaltene Logik gilt sowohl während des Entwurfs, wenn Sie die Aktivität zu einer Arbeitsablaufdefinition hinzufügen, als auch bei Ausführung, wenn eine Arbeitsablaufinstanz ausgeführt wird. Wenn die Ausführung alle Aktivitäten in einem bestimmten Flusspfad abgeschlossen ist, ist die Arbeitsablaufinstanz abgeschlossen.

Arbeitsablauf-Designer (Workflow Designer)

Der Workflow Designer ist ein von Quest One ActiveRoles für die Erstellung von Arbeitsabläufen bereitgestelltes grafisches Tool. Das Tool stellt die Arbeitsablaufdefinition als ein Prozessdiagramm mit Symbolen, die Arbeitsablaufaktivitäten angeben, und direktionalen Pfeilen, die die Übergänge zwischen den Aktivitäten angeben, dar. Benutzer ziehen Aktivitäten vom Aktivitätsbereich auf das Prozessdiagramm und konfigurieren sie mit Hilfe der von der Designer-Schnittstelle bereitgestellten Seiten. Für die Konfiguration der Arbeitsablauf-Startbedingungen stehen separate Seiten zur Verfügung.

Arbeitsablauf-Modul

Quest One ActiveRoles nutzt das Laufzeitmodul von Microsoft Windows Workflow Foundation für die Erstellung und Pflege von Arbeitsablaufinstanzen. Das Modul unterstützt mehrere, parallel ausgeführte Arbeitsablaufinstanzen. Wenn ein Arbeitsablauf gestartet wird, überwacht das Modul den Status der Arbeitsablaufinstanz, koordiniert die Weiterleitung der Aktivitäten in der Arbeitsablaufinstanz, bestimmt, welche Aktivitäten für die Ausführung ausgewählt werden dürfen, und führt Aktivitäten aus. Das Arbeitsablauf-Modul wird im Prozess mit dem Verwaltungsdienst gehostet, der bei Laufzeit Arbeitsabläufen die Kommunikation mit Quest One ActiveRoles ermöglicht.

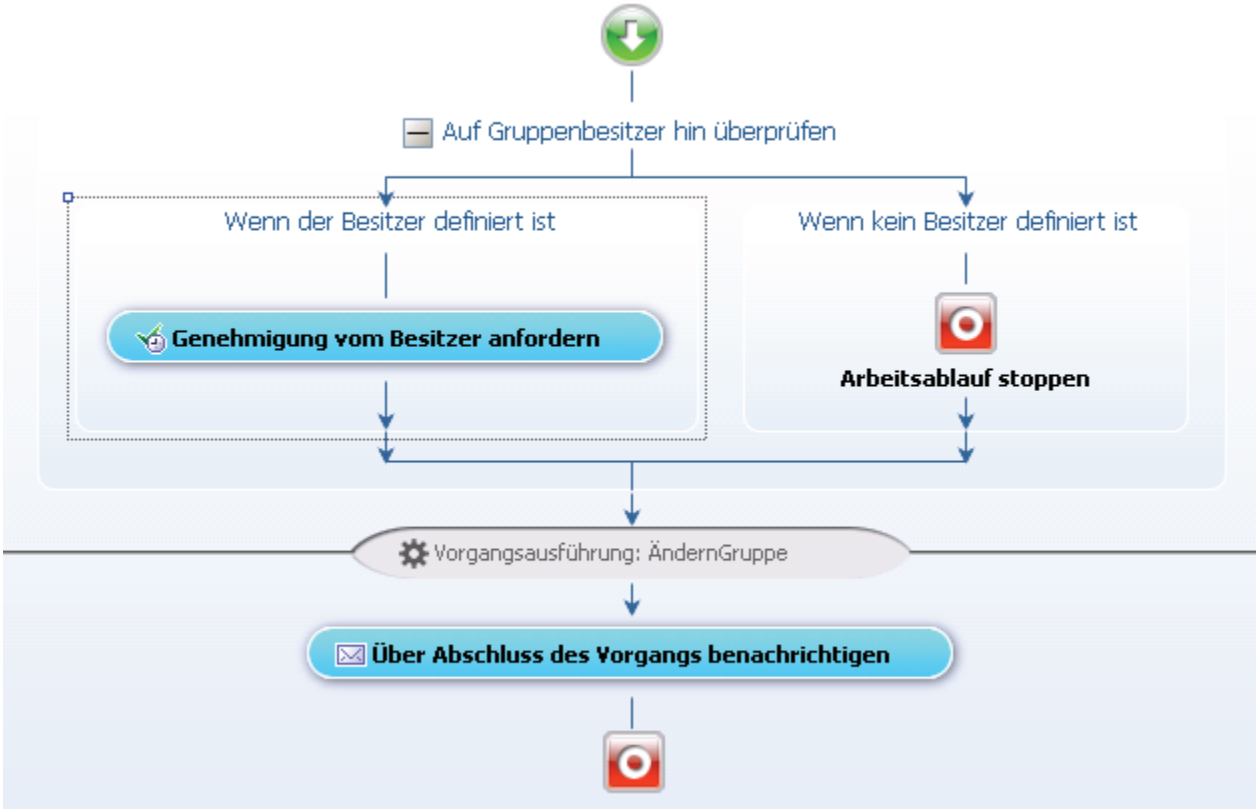
E-Mail-Benachrichtigungen

Benutzer werden per E-Mail über bestimmte, innerhalb eines Arbeitsablaufs eintretende Situation benachrichtigt. Eine Benachrichtigungsmeldung wird generiert und an die angegebenen Empfänger gesendet, um sie über den Eintritt eines bestimmten Ereignisses wie etwa das Senden einer neuen Genehmigungsaufgabe an die genehmigenden Instanzen oder den Abschluss des Vorgangs zu informieren. Eine Benachrichtigungskonfiguration umfasst solche Elemente wie etwa das Ereignis, bei dessen Eintritt eine Benachrichtigung erfolgen soll, die Liste der Benachrichtigungsempfänger und die Vorlage für die Benachrichtigungsmeldung.

Arbeitsablaufprozesse

Die Logik eines automatisierten Verwaltungsprozesses kann mit Hilfe von administrativen Richtlinien in Quest One ActiveRolesr implementiert werden. Die Erstellung und Pflege komplexer, mehrere Schritte umfassender Prozesse auf diese Weise kann jedoch eine große Herausforderung darstellen. Arbeitsabläufe bieten einen anderen Ansatz. Sie ermöglichen IT-Administratoren die grafische Definition eines Verwaltungsprozesses. Dies kann schneller als die Erstellung des Prozesses durch Anwendung einzelner Richtlinien sein. Außerdem ist der Prozess so verständlicher, leichter zu erläutern und zu ändern.

Das Diagramm unten zeigt einen in der Quest One ActiveRoles-Konsole erstellten Arbeitsablauf. In diesem einfachen Beispiel überprüft der Arbeitsablauf bei einer Anforderung zum Hinzufügen eines Benutzers zu einer bestimmten Gruppe zunächst, ob die Gruppe über einen Besitzer verfügt. Wenn die Gruppe über keinen Besitzer verfügt, werden die angeforderten Änderungen verweigert, und der Arbeitsablauf ist abgeschlossen; andernfalls werden die Änderungen zur Genehmigung an den Besitzer der Gruppe weitergeleitet. Nach Erhalt der Genehmigung wendet Quest One ActiveRoles die Änderungen an und fügt den Benutzer zur Gruppe hinzu. Im Prozessdiagramm wird dieser Schritt als **Vorgangsausführung** bezeichnet. Wenn der Besitzer die Änderungen ablehnt, wird der Arbeitsablauf beim vorigen (Genehmigungs-) Schritt beendet, sodass die Änderungen nicht übernommen werden. Nach der Durchführung der Änderungen sendet der Arbeitsablauf eine E-Mail-Benachrichtigung an die Person, die die Änderungen angefordert hat, und wird dann beendet.



Im Beispiel oben verwaltet der Arbeitsablauf den Prozess des Hinzufügens eines Benutzers zu einer Gruppe gemäß den zum Zeitpunkt des Entwurfs des Arbeitsablaufs definierten Regeln. Die Regeln stellen die Arbeitsablaufdefinition dar und umfassen die Aktivitäten, die innerhalb des Prozesses durchgeführt werden, sowie die Beziehungen zwischen den Aktivitäten. Eine Aktivität in einer Prozessdefinition kann eine standardmäßig verfügbare, vordefinierte Funktion wie etwa eine Genehmigungsanforderung oder eine Benachrichtigung über Bedingungen, die das Eingreifen des Benutzers erfordern, oder eine benutzerdefinierte Funktion, die mit Hilfe von Skripttechnologien erstellt wurde, sein.

Ein Arbeitsablaufprozess wird gestartet, wenn die angeforderten Änderungen den in der Arbeitsablaufdefinition angegebenen Bedingungen entsprechen. Im Beispiel oben können die Bedingungen so eingerichtet werden, dass der Arbeitsablauf immer dann startet, wenn ein Benutzer von Quest One ActiveRoles Änderungen an der Mitgliedschaftsliste einer bestimmten Gruppe vorgenommen hat. Wenn die Bedingungen erfüllt sind, startet der Arbeitsablaufprozess, um die Änderungen durch die Arbeitsablaufdefinition zu leiten. Hierbei führt er automatisierte Schritte durch und fordert bei Bedarf eine Aktion von einer Person (wie etwa eine Genehmigung) an.

Übersicht über die Arbeitsablaufverarbeitung

In Quest One ActiveRoles werden Verzeichnisobjekte wie etwa Benutzer, Gruppen oder Computer vom Verwaltungsdienst verwaltet. Diese Objekte können über Anforderungen, die an den Verwaltungsdienst gerichtet werden, erstellt, geändert oder gelöscht werden. Jede Anforderung startet einen Vorgang, um die angeforderten Änderungen an den Verzeichnisdaten vorzunehmen. So startet zum Beispiel eine Anforderung zur Erstellung eines Benutzers oder einer Gruppe den Erstellungsvorgang, wobei der Zielobjekttyp auf „Benutzer" bzw. „Gruppe" gesetzt ist; Eine Anforderung zum Hinzufügen von Benutzern zu einer Gruppe startet den Vorgang „Ändern" für diese Gruppe.

Wenn ein Vorgang gestartet wurde, startet der Verwaltungsdienst die Verarbeitung des Vorgangs. Jeder Vorgang wird durch ein einzelnes Objekt angegeben, das normalerweise als das Anforderungsobjekt bezeichnet wird und das alle für die Durchführung des Vorgangs erforderlichen Informationen enthält. Daher durchläuft das Anforderungsobjekt im Rahmen der Vorgangsverarbeitung eine Reihe von Phasen innerhalb des Verwaltungsdienstes.

Das Vorgangsverarbeitungsmodell in Quest One ActiveRoles besteht aus vier Hauptphasen: Zugriffskontrolle, Vorausführung, Ausführung und Nachausführung. Das Anforderungsobjekt durchläuft diese Phasen in der folgenden Reihenfolge:

- **Zugriffskontrolle.** In dieser Phase überprüft der Verwaltungsdienst, ob der Benutzer oder das System, der bzw. das die Anforderung gestellt hat, über ausreichende Rechte zur Durchführung der angeforderten Änderungen verfügt. Bei unzureichenden Rechten wird der Vorgang verweigert.
- **Vorausführung.** Während dieser Phase führt der Verwaltungsdienst zunächst die Vorausführungs-Arbeitsablaufaktivitäten aus. Dies sind die Aktivitäten, die sich im oberen Teil des Arbeitsablaufprozessdiagramms über der Zeile **Vorgangsausführung** befinden. Ein typisches Beispiel sind Genehmigungsaktivitäten: An diesem Punkt können die genehmigenden Instanzen den Vorgang zulassen oder ablehnen.

  Wenn die Vorausführungsaktivitäten abgeschlossen wurden, ohne dass der Vorgang zurückgewiesen wurde, führt der Verwaltungsdienst die Vorausführungsrichtlinien aus. Typische Beispiele für solche Richtlinien umfassen die Erstellung von Eigenschaften und Bestätigungsregeln sowie die Funktionen, die so genannte „Vorereignis-Handler" in Skriptrichtlinien implementieren.
- **Ausführung.** In dieser Phase führt der Verwaltungsdienst den Vorgang aus und nimmt die angeforderten Änderungen an den Verzeichnisdaten vor. Wenn beispielsweise die Erstellung eines Benutzers angefordert ist, wird der Benutzer in dieser Phase erstellt.

- **Nachausführung.** Während dieser Phase führt der Verwaltungsdienst zunächst die Nachausführungsrichtlinien aus. So erfolgt zum Beispiel bei der Erstellung eines Benutzers in dieser Phase die Bereitstellung eines Stammordners oder von Gruppenmitgliedschaften für diesen Benutzer. Die Funktionen, die „Nachereignis-Handlers" in Skriptrichtlinien implementieren, werden ebenfalls in diesem Schritt ausgeführt.

  Schließlich führt der Verwaltungsdienst nach beendeter Ausführung der Nachausführungsrichtlinien die Nachausführungs-Arbeitsablaufaktivitäten aus. Dies sind die Aktivitäten, die sich im unteren Teil des Arbeitsablaufprozessdiagramms unter der Zeile **Vorgangsausführung** befinden. Ein typisches Beispiel sind Benachrichtigungsaktivitäten, die E-Mails versenden, die über den Abschluss des Vorgangs informieren.

Der Verwaltungsdienst führt die Arbeitsablaufaktivitäten nacheinander in der im Arbeitsablaufprozessdiagramm gezeigten sequenziellen Reihenfolge aus, bis die letzte Aktivität beendet ist. Wenn-Dann-Sonst-Aktivitäten können verwendet werden, um eine bedingte Verzweigung in Arbeitsabläufen zu erreichen. Diese Verzweigungen ermöglichen die Änderung der Reihenfolge von Aktivitäten abhängig von den an der Anforderung involvierten Daten.

Zu Beginn der Vorausführungsphase legt der Verwaltungsdienst die zu startenden Arbeitsabläufe fest. Die Anforderung wird mit allen vorhandenen Arbeitsablaufdefinitionen verglichen. Damit ein Arbeitsablauf startet, muss der angeforderte Vorgang die für diesen Arbeitsablauf definierten Startbedingungen erfüllen. Wenn die Startbedingungen erfüllt sind wird der Arbeitsablauf an die Anforderung angepasst.

Für einen Arbeitsablauf, der an die Anforderung angepasst wird, führt der Verwaltungsdienst die Aktivitäten aus, die in diesem Arbeitsablauf während der entsprechenden Phasen der Vorgangsverarbeitung gefunden wurden. Nur ein Arbeitsablauf oder mehrere Arbeitsabläufe können an eine einzelne Anforderung angepasst werden. Bei mehreren Arbeitsabläufen startet der Verwaltungsdienst jeden dieser Abläufe einzeln nacheinander und führt zunächst alle in diesen Arbeitsabläufen enthaltenen Vorausführungsaktivitäten aus. Dann führt der Verwaltungsdienst während der Nachausführungsphase alle in diesen Arbeitsabläufen enthaltenen Nachausführungsaktivitäten aus.

Werden mehrere Arbeitsabläufe an eine einzelne Anforderung angepasst, verwendet ActiveRoles das Attribut `edsaWorkflowPriority` des Arbeitsablaufdefinitionsobjekts, um die Reihenfolge der Ausführung der Arbeitsabläufe festzulegen. Die Aktivitäten des Arbeitsablaufs mit einem niedrigeren Wert dieses Attributs werden vor den Aktivitäten des Arbeitsablaufs mit einem höheren Wert dieses Attributs ausgeführt. Arbeitsabläufe mit gleichem Prioritätswert werden in aufsteigender Reihenfolge nach den Namen der Arbeitsabläufe ausgeführt. Das Attribut `edsaWorkflowPriority` ist standardmäßig auf 500 gesetzt. Ist das Attribut `edsaWorkflowPriority` nicht gesetzt, geht ActiveRoles von einem Prioritätswert von 500 aus. Sie können den Wert des Attributs `edsaWorkflowPriority` ändern, um sicherzustellen, dass ein bestimmter Arbeitsablauf vor anderen Arbeitsabläufen ausgeführt wird. Ein niedriger Wert des Attributs bedeutet eine höhere Priorität, und ein höherer Wert bedeutet eine niedrigere Priorität. Sie können das Attribut `edsaWorkflowPriority` anzeigen oder ändern, indem Sie den Befehl **Erweiterte Eigenschaften** auf das Arbeitsablaufdefinitionsobjekt in der ActiveRoles-Konsole anwenden.

Startbedingungen

Um einen Arbeitsablauf in Quest One ActiveRoles bereitzustellen, erstellen Sie eine Arbeitsablaufdefinition, konfigurieren dann die Startbedingungen für diesen Arbeitsablauf, fügen Arbeitsablaufaktivitäten hinzu und konfigurieren diese. Bei der Konfiguration von Arbeitsablauf-Startbedingungen geben Sie Folgendes an:

- Vorgangstyp wie etwa „Erstellen", „Umbenennen", „Ändern" oder „Löschen"; der Arbeitsablauf wird nur dann an die Anforderung angepasst, wenn ein Vorgang dieses Typs angefordert ist.

- Objekttyp wie etwa „Benutzer", „Gruppe" oder „Computer"; der Arbeitsablauf wird nur dann an die Anforderung angepasst, wenn der Vorgang Änderungen an einem Objekt dieses Typs anfordert.
- Für den Vorgangstyp „Ändern" eine Liste der Objekteigenschaften; der Arbeitsablauf wird nur dann an die Anforderung angepasst, wenn der Vorgang Änderungen an irgendeiner dieser Eigenschaften eines Objekts anfordert.
- Identität eines Vorgangsanforderers (Initiator) wie etwa ein Benutzer, eine Gruppe oder ein Dienst; der Arbeitsablauf wird nur dann an die Anforderung angepasst, wenn der Vorgang im Namen dieser Identität angefordert wird.
- Container wie etwa eine Organisationseinheit oder eine verwaltete Einheit; der Arbeitsablauf wird nur dann an die Anforderung angepasst, wenn der Vorgang Änderungen an bzw. die Erstellung von einem Objekt in diesem Container anfordert.
- Optional ein Filter, der alle zusätzlichen Bedingungen für die an einem Vorgang beteiligten Einheiten definiert; der Arbeitsablauf wird nur dann an die Anforderung angepasst, wenn der Vorgang diesen Bedingungen entspricht. Wenn kein Filter festgelegt ist, dann sind keine zusätzlichen Bedingungen gültig.

Bei einer Anforderung für einen beliebigen Vorgang, die alle für einen Arbeitsablauf angegebenen Startbedingungen erfüllt, passt der Verwaltungsdienst den Arbeitsablauf an die Anforderung an und führt die im Arbeitsablauf gefundenen Aktivitäten aus.

Übersicht über die Arbeitsablaufaktivitäten

Aktivitäten sind Arbeitseinheiten, von denen jede zur Erfüllung eines Arbeitsablaufprozesses beiträgt. Quest One ActiveRoles bietet eine Standardreihe von Aktivitäten, die eine vordefinierte Funktion für die Genehmigung, Benachrichtigung, den Kontrollfluss und Bedingungen ausführen. Damit eine Aktivität benutzerdefinierte Funktionen ausführt, können Skripts erstellt werden.

Aktivitäten sind die wesentlichen Bausteine für Arbeitsabläufe. Ein Arbeitsablauf ist im Grunde eine Reihe von Aktivitäten, die in einem Prozessdiagramm zusammengefasst sind. Wenn Sie einen Arbeitsablauf mit Hilfe des Workflow Designers errichten, ziehen Sie Aktivitäten aus dem Aktivitätsbereich auf das Prozessdiagramm und konfigurieren sie dann dort. Die für alle Aktivitäten geltenden konfigurierbaren Einstellungen lauten:

- **Name.** Der Name wird verwendet, um die Aktivität im Arbeitsablaufdiagramm zu identifizieren.
- **Beschreibung.** Dieser optionale Text ist nützlich für die Unterscheidung der Aktivitäten. Die Beschreibung wird angezeigt, wenn Sie mit der Maus auf die entsprechende Aktivität im Prozessdiagramm zeigen.

In den folgenden Abschnitten sind die Aktivitätstypen beschrieben, die in Quest One ActiveRoles enthalten sind. Die Abschnitte enthalten Informationen zu den für jeden Aktivitätstyp spezifischen, konfigurierbaren Einstellungen.

Genehmigungsaktivität

Eine Genehmigungsaktivität, auch als „Genehmigungsregel" bezeichnet, stellt einen Entscheidungspunkt in einem Arbeitsablauf auf, der verwendet wird, um die Autorisierung von einer Person zu erhalten, bevor der Arbeitsablauf fortgesetzt werden kann. Die Arbeitsablauf-Startbedingungen geben an, welche Vorgänge den Arbeitsablauf starten. Die zum Arbeitsablauf hinzugefügten Genehmigungsregeln bestimmen, wer den Vorgang genehmigen soll, in welcher Reihenfolge die Genehmigungen erfolgen sollen und wer über Genehmigungsaufgaben oder Entscheidungen benachrichtigt werden soll.

Quest One ActiveRoles erstellt eine Genehmigungsaufgabe als Teil der Verarbeitung einer Genehmigungsregel und weist die Aufgabe dann genehmigenden Instanzen zu. Von der genehmigenden Instanz wird die Erfüllung der Aufgabe erwartet, d.h. sie muss die Entscheidung treffen, ob der Vorgang zulässig ist oder abgelehnt werden soll. Bis zum Abschluss der Aufgabe verbleibt der Vorgang im Status „Ausstehend".

Die folgenden Themen behandeln die spezifischen, für eine Genehmigungsaktivität konfigurierbaren Einstellungen.

Genehmigende Instanzen und Eskalation

Genehmigende Instanzen sind die Benutzer oder Benutzergruppen, die berechtigt sind, Genehmigungsaufgaben durchzuführen. Bei der Verarbeitung einer Genehmigungsregel erstellt Quest One ActiveRoles eine Genehmigungsaufgabe und weist sie dann den von der Regel definierten genehmigenden Instanzen zu. Der Status der Aufgabe bestimmt den Übergang des Arbeitsablaufs: die Aufgabe muss die Auflösung „Genehmigen" erhalten, damit der Vorgang der Genehmigungsregel entspricht. Wenn der Aufgabe die Auflösung „Zurückweisen" zugewiesen wird, wurde der Vorgang verweigert, und die Arbeitsablaufinstanz ist abgeschlossen.

Genehmigende Instanzen können per Suche in den verfügbaren Benutzern und Gruppen ausgewählt werden. Es können auch bestimmte Funktionsinhaber als genehmigende Instanzen benannt werden. So kann zum Beispiel eine Genehmigungsregel so konfiguriert werden, dass die Genehmigung durch den Vorgesetzten der Person, die den Vorgang angefordert hat, oder vom Vorgesetzten der Gruppe oder des Containers, die bzw. der von diesem Vorgang betroffen ist, erfolgen muss.

Mit einer Genehmigungsregel können zwei oder mehr Ebenen genehmigender Instanzen definiert werden, die jeweils eigene Listen genehmigender Instanzen umfassen. Quest One ActiveRoles verwendet Ebenen genehmigender Instanzen zur Eskalation zeitlich begrenzter Genehmigungsaufgaben. Für jede Ebene genehmigender Instanzen kann eine bestimmte Zeitdauer festgelegt werden. Wird die Genehmigungsaufgabe von einer genehmigenden Instanz nicht innerhalb der festgelegten Zeitdauer abgeschlossen, kann Quest One ActiveRoles die Aufgabe den genehmigenden Instanzen der nächsthöheren Ebene zuweisen. Dieser Prozess wird als *Eskalation* bezeichnet.

Jede Genehmiger-Ebene verfügt über die folgenden Konfigurationsoptionen:

- **Liste der Genehmiger.** Gibt die Benutzer oder Benutzergruppen an, die als Genehmiger für die betreffende Genehmiger-Ebene festgelegt sind.

  Damit eine Genehmigungsrichtlinie gültig ist, muss mindestens eine Liste der Genehmiger für die erste Genehmigungsebene angegeben werden. Quest One ActiveRoles weist die Genehmigungsaufgabe zunächst dem Genehmiger dieser Ebene zu. Um die Eskalation zu ermöglichen, muss eine separate Genehmiger-Liste für ein oder mehrere Eskalationsebenen angegeben werden.

- **Die Genehmigungsaufgabe hat keine Frist.** Wenn diese Option ausgewählt ist, erfordert die Genehmigungsregel nicht, dass die Genehmiger der entsprechenden Ebene die Genehmigungsaufgabe innerhalb einer bestimmten Frist abschließen.
- **Die Genehmigungsaufgabe hat eine Frist von**<*Anzahl*> **Tage** <*Anzahl*> **Stunden.** Wenn diese Option ausgewählt ist, erfordert die Genehmigungsregel, dass die Genehmiger der entsprechenden Ebene die Genehmigungsaufgabe innerhalb des angegebenen Zeitraums abschließen.

  Wenn die Genehmigungsaufgabe nicht innerhalb des angegebenen Zeitraums abgeschlossen wird, dann kann die Genehmigungsregel abhängig von der ausgewählten Konfigurationsoption entweder den zur Genehmigung anstehenden Vorgang abbrechen oder die Genehmigungsaufgabe eskalieren. Die letztgenannte Option erfordert, dass eine Liste der Genehmiger für die nachfolgende Eskalationsebene angegeben ist.

- **Zulassen, dass die genehmigende Instanz die Genehmigungsaufgabe delegiert.** Wenn diese Option ausgewählt ist, darf der Genehmiger der entsprechenden Ebene die Genehmigungsaufgabe anderen Personen zuweisen. Auf den Seiten zur Durchführung der Genehmigungsaufgabe kann der Genehmiger die Schaltfläche **Delegieren** verwenden, um die Personen auszuwählen, denen er die Aufgabe zuweisen möchte.
- **Zulassen, dass die genehmigende Instanz die Genehmigungsaufgabe eskaliert.** Wenn diese Option ausgewählt ist, darf der Genehmiger der entsprechenden Ebene die Genehmigungsaufgabe eskalieren. Auf den Seiten zur Durchführung der Genehmigungsaufgabe kann der Genehmiger die Schaltfläche **Eskalieren** verwenden, um die Aufgabe den Genehmigern der nächsten Eskalationsebene zuzuweisen. Diese Option erfordert, dass eine Liste der Genehmiger für die nachfolgende Eskalationsebene angegeben ist.

Informationsanfrage

Sie können die Genehmigungsaktivität so konfigurieren, das die genehmigende Instanz aufgefordert wird, im Rahmen der Genehmigungsaufgabe bestimmte Eigenschaften des Objekts zu liefern. Angenommen, die Erstellung eines Benutzers wird zur Genehmigung gesendet. Die genehmigende Instanz kann aufgefordert werden, neben den in der Erstellungsanforderung genannten Eigenschaften bestimmte Eigenschaften des Benutzers anzugeben. Damit können Sie die Genehmigungsaktivität so konfigurieren, dass die genehmigende Instanz aufgefordert wird, die Postfachdatenbank für das Postfach des zu erstellenden Benutzers anzugeben.

Die Genehmigungsaktivität kann auch so konfiguriert werden, dass die zur Genehmigung eingereichten Objekteigenschaften von der genehmigenden Instanz überprüft werden müssen. Eine weitere Option kann sein, dem Genehmiger zu gestatten, Änderungen an diesen Eigenschaften vorzunehmen.

Die Seiten zur Konfiguration einer Genehmigungsaktivität in der ActiveRoles-Konsole umfassen die folgenden Optionen im Zusammenhang mit der Anforderung von Informationen:

- **Der genehmigenden Instanz diese Anweisung zeigen.** Bei der Ausführung der Genehmigungsaufgabe sieht die genehmigende Instanz diese Anweisung auf der Seite, auf welcher die Eigenschaften, die der Genehmigungsaufgabe unterstehen, geprüft, angegeben oder geändert werden können. Es kann eine Anweisung über die Art der Ausführung der Aufgabe angegeben werden.
- **Die genehmigende Instanz auffordern, diese Eigenschaften anzugeben oder zu ändern.** Bei der Ausführung der Genehmigungsaufgabe wird die genehmigende Instanz aufgefordert, die in dieser Option aufgeführten Eigenschaften anzugeben oder zu ändern.
- **Der genehmigenden Instanz die ursprüngliche Anforderung zeigen.** Diese Option fügt auf den Seiten, auf welchen die Genehmigungsaufgabe ausgeführt wird, einen separater Abschnitt hinzu, in dem die zur Genehmigung eingereichten Eigenschaften aufgeführt werden.
- **Zulassen, dass die genehmigende Instanz die ursprüngliche Anforderung ändert.** Sofern diese Option nicht ausgewählt ist, darf die genehmigende Instanz die zur Genehmigung eingereichten Eigenschaften lediglich einsehen. Aktivieren Sie dieses Kontrollkästchen, damit die genehmigende Instanz diese Eigenschaften ändern kann.

Anpassung

Sie können die Genehmigungsaktivität so konfigurieren, dass angegeben wird, wie die von dieser Aktivität erstellten Genehmigungsaufgaben im Abschnitt „Genehmigung" des Web-Interface identifiziert werden sollen. Der Abschnitt „Genehmigung" enthält eine Liste der Genehmigungsaufgaben, wobei jede Aufgabe durch eine Kopfzeile identifiziert ist, die Basisinformationen über die Aufgabe einschließlich des Titels der Aufgabe und Informationen über das Zielobjekt des zur Genehmigung eingereichten Vorgangs enthält. Der Titel der Aufgabe ist in der Mitte der Kopfzeile der Aufgabe aufgeführt. Die Eigenschaften, die das Zielobjekt des Vorgangs angeben, werden über dem Titel der Aufgabe angezeigt.

Die Seiten für die Konfiguration einer Genehmigungsaktivität in der ActiveRoles-Konsole enthalten die folgenden mit der Kopfzeile der Genehmigungsaufgabe in Verbindung stehenden Anpassungsoptionen:

- **Diese Bezeichnung zeigen, um die Genehmigungsaufgabe zu erkennen.** Bei der Ausführung der Genehmigungsaufgabe sieht die genehmigende Instanz diese Anweisung auf der Seite, auf welcher die Eigenschaften, die der Genehmigungsaufgabe unterstehen, geprüft, angegeben oder geändert werden können. Es kann eine Anweisung über die Art der Ausführung der Aufgabe angegeben werden.

- **Diese Eigenschaften des zur Genehmigung eingereichten Objekts anzeigen.** Diese Eigenschaften werden in der Kopfzeile der Aufgabe auf den Seiten angezeigt, auf welchen die Genehmigungsaufgabe ausgeführt wird. Es können Eigenschaften hinzugefügt werden, die der genehmigenden Instanz helfen, das Zielobjekt des genehmigungspflichtigen Vorgangs zu erkennen.
- **Die Vorgangsübersicht im Aufgabenkopf anzeigen.** Diese Option erweitert die Kopfzeile der Genehmigungsaufgabe dahingehend, dass eine Informationsübersicht über die genehmigungspflichtigen Änderungen einschließlich der Änderungen und ihrer Begründung gegeben wird.

Sie können die Genehmigungsaktivität so konfigurieren, dass die Aktionen angegeben werden, die die genehmigende Instanz an der Genehmigungsaufgabe ausführen kann. Auf den Seiten zur Durchführung der Genehmigungsaufgabe im Abschnitt „Genehmigung" des Web-Interface enthält die Kopfzeile der Aufgabe die Aktionsschaltflächen, die zur Anwendung der entsprechenden Lösung auf die Aufgabe vorgehen sind (z. B. **Genehmigen** oder **Ablehnen**). Die Aktionsschaltflächen werden unten in der Kopfzeile angezeigt. Welche Schaltflächen angezeigt werden, ist von der Konfiguration der Genehmigungsaktivität abhängig.

Auf den Seiten zum Konfigurieren einer Genehmigungsaktivität auf der ActiveRoles-Konsole finden Sie folgende Optionen zur Anpassung von Aktionsschaltflächen:

- **Aktionsschaltfläche konfigurieren.** Die Aktionsschaltflächen sind auf den Seiten für die Ausführung der Genehmigungsaufgabe aufgeführt. Jede Schaltfläche ordnet der Aufgabe eine bestimmte Aktion zu. Standardmäßig werden zwei integrierte Schaltflächen mit den Bezeichnungen **Genehmigen** und **Ablehnen** für jede Genehmigungsaufgabe angezeigt. Je nach Konfiguration der Genehmigungsaktivität können auch andere Schaltflächen angezeigt werden. Es können Schaltflächen für die Erstellung benutzerdefinierter Aktionen hinzugefügt werden. Abhängig vom Aktionstyp der Schaltfläche führt das Anklicken einer benutzerdefinierten Aktionsschaltfläche dazu, dass der Arbeitsablauf den zur Genehmigung anstehenden Vorgang zulässt (Aktionstyp „Abschließen") oder ablehnt (Aktionstyp „Ablehnen"). Wenn-Dann-Aktivitäten können je nach Bezeichnung der Schaltfläche auf eine benutzerdefinierte Aktionsschaltfläche verweisen und den geeigneten Teil des Arbeitsablaufs wählen, wenn die genehmigende Instanz diese benutzerdefinierte Aktionsschaltfläche anklickt.
- **Diese Anweisung für die Aktionsschaltflächen zeigen.** Verwenden Sie diese Option, um eine Anweisung über die Art der Verwendung der Aktionsschaltflächen anzugeben. Die genehmigende Instanz sieht diese Anweisung über den Aktionsschaltflächen auf den Seiten, auf welchen die Genehmigungsaufgabe ausgeführt wird.
- **Den Bestätigungsdialog bei Abschluss der Genehmigungsaufgabe löschen.** Wenn diese Option nicht ausgewählt ist, fordert ActiveRoles die genehmigende Instanz auf, jedes Mal, wenn die genehmigende Instanz eine Genehmigungsaufgabe durchführt, ein Bestätigungs-Dialogfeld auszufüllen. Sie können diese Option auswählen, um zu verhindern, dass das Bestätigungs-Dialogfeld angezeigt wird, so dass die genehmigende Instanz die Aufgabe abschließen kann, ohne einen Grund für die Fertigstellung der Aufgabe angeben zu müssen.

Benachrichtigung

„Benachrichtigung" wird verwendet, um Empfänger als Abonnenten der Benachrichtigungen über Ereignisse im Zusammenhang mit der Genehmigung festzulegen, um Benachrichtigungs-E-Mails zu konfigurieren und um die E-Mail-Übertragung einzurichten. Genehmigungsregeln ermöglichen in Verbindung mit verschiedenen Ereignissen wie etwa der Erstellung von Genehmigungsaufgaben

bei Vorgangsanforderungen die Benachrichtigung von Arbeitsablauf-Benutzern per E-Mail. So können genehmigende Instanzen über die Anforderungen, die durch sie genehmigt werden sollen, per E-Mail einschließlich Hypertext-Verknüpfungen zu dem mit der Genehmigung verbundenen Bereich im Web-Interface benachrichtigt werden. Eine Genehmigungsaktivität hat die folgenden Benachrichtigungseinstellungen:

Benachrichtigungsempfänger

„Benachrichtigungsempfänger" sind die Benutzer oder Gruppen, an die die Aktivität E-Mails sendet. Ein Empfänger kann jeder beliebige Postfach-fähige Benutzer oder jede E-Mail-fähige Gruppe sein. Es gibt auch eine Reihe von Optionen, die es Ihnen ermöglichen, Empfänger auf der Grundlage ihrer Funktion wie etwa einen Vorgangsanforderer, eine genehmigende Instanz, einen Vorgesetzten des Vorgangsanforderers oder einen Verwalter des von dem Vorgang betroffenen Objekts auszuwählen.

Benachrichtigungsübermittlung

Die Übermittlungsoptionen legen fest, ob Benachrichtigungen sofort oder gemäß Zeitplan gesendet werden. Die Option der sofortigen Übermittlung führt dazu, dass die Aktivität bei jedem Eintritt des Ereignisses, bei dem eine Benachrichtigung erfolgen soll, eine separate Nachricht generiert. Die Option der geplanten Übermittlung kann für die Sammlung von Benachrichtigungen verwendet werden. Wenn Sie sich für eine geplante Übermittlung entschließen, werden alle Benachrichtigungen über den Eintritt des Ereignisses innerhalb eines frei wählbaren Zeitraums gesammelt und als eine einzige Nachricht gesendet.

Benachrichtigungsmeldung

Benachrichtigungsmeldungen basieren auf einer Nachrichtenvorlage, die das Format und den Inhalt von E-Mail-Benachrichtigungen einschließlich des Nachrichtenbetreffs und Nachrichtentexts festlegt. Eine Vorlage ist ein Dokument im HTML-Format, das Sie anzeigen und bei Bedarf ändern können, um Benachrichtigungsmeldungen anzupassen. Der Vorlagentext kann dynamischen Inhalt umfassen, der bei Laufzeit durch Abfrage von Informationen aus der ausgeführten Instanz des Arbeitsablaufprozesses generiert wird.

Web-Interface-Adresse

Mit der Einstellung „Web-Interface-Adresse" wird die Adresse (URL) des Quest One ActiveRoles-Web-Interface angegeben. Diese Einstellung wird von der Aktivität verwendet, um Hyperlinks in den Benachrichtigungsmeldungen zu erstellen.

E-Mail-Server

Mit der Einstellung „E-Mail-Server" werden der Name und andere Parameter des E-Mail-Servers angegeben, die zur Übermittlung von Benachrichtigungsmeldungen verwendet werden.

Benachrichtigungsaktivität

Eine Benachrichtigungsaktivität in einem Arbeitsablauf wird verwendet, um Empfänger als Abonnenten von Benachrichtigungen über folgende Ereignisse festzulegen:

- **Bei der Ausführung dieser Aktivität.** Dieses Ereignis tritt bei Ausführung der Benachrichtigungsaktivität auf. Wenn die Option so konfiguriert ist, dass bei Eintritt dieses Ereignisses eine Benachrichtigung erfolgen soll, dann erstellt die Aktivität eine E-Mail, die über die Ausführung der Benachrichtigungsaktivität informiert, und sendet diese sofort. Die Benachrichtigung über dieses Ereignis dient normalerweise dazu, darüber zu informieren, dass der Arbeitsablauf-Ausführungsvorgang die Benachrichtigungsaktivität erreicht hat.
- **Arbeitsablauf erfolgreich abgeschlossen.** Wenn die Option so konfiguriert ist, dass bei Eintreten dieses Ereignisses eine Benachrichtigung erfolgen soll, erstellt die Aktivität eine Nachricht, die bei Abschluss des Arbeitsablaufs gesendet werden soll. Wenn der Arbeitsablauf abgeschlossen ist, sendet ActiveRoles diese Nachricht, wenn während der Ausführung des Arbeitsablaufs keine schweren Fehler aufgetreten sind.
- **Der Arbeitsablauf hat einen Fehler festgestellt.** Wenn die Option so konfiguriert ist, dass bei Eintreten dieses Ereignisses eine Benachrichtigung erfolgen soll, erstellt die Aktivität eine Nachricht, die bei Abschluss des Arbeitsablaufs gesendet werden soll. Wenn der Arbeitsablauf abgeschlossen ist, sendet ActiveRoles diese Nachricht, wenn während der Ausführung des Arbeitsablaufs einige Fehler aufgetreten sind.
- **Vorgang ausgeführt.** Wenn die Option so konfiguriert ist, dass bei Eintreten dieses Ereignisses eine Benachrichtigung erfolgen soll, erstellt die Aktivität eine Nachricht, die bei Abschluss des Arbeitsablaufs gesendet werden soll. Wenn der Arbeitsablauf abgeschlossen ist, sendet ActiveRoles diese Nachricht, wenn der Vorgang, der den Arbeitsablauf ausgelöst hat, erfolgreich ausgeführt wurde.

Die Konfiguration einer Benachrichtigungsaktivität gibt das Ereignis, über das benachrichtigt werden soll, sowie die Benachrichtigungsempfänger an. Bei Ausführung durch den Arbeitsablauf bereitet die Benachrichtigungsaktivität eine dem angegebenen Ereignis entsprechende Benachrichtigungsmeldung vor. ActiveRoles hält die von der Aktivität vorbereitete Meldung zurück und sendet die Meldung bei Eintritt des Ereignisses an die angegebenen Empfänger. Die für eine Benachrichtigungsaktivität konfigurierbaren Einstellungen sind identisch mit den Benachrichtigungseinstellungen einer Genehmigungsaktivität. Sie sind nachfolgend aufgeführt.

Benachrichtigungsempfänger

„Benachrichtigungsempfänger" sind die Benutzer oder Gruppen, an die die Aktivität E-Mails sendet. Ein Empfänger kann jeder beliebige Postfach-fähige Benutzer oder jede E-Mail-fähige Gruppe sein. Es gibt auch eine Reihe von Optionen, die es Ihnen ermöglichen, Empfänger auf der Grundlage ihrer Funktion wie etwa einen Vorgangsanforderer, eine genehmigende Instanz, einen Vorgesetzten des Vorgangsanforderers oder einen Verwalter des von dem Vorgang betroffenen Objekts auszuwählen.

Benachrichtigungsmeldung

Benachrichtigungsmeldungen basieren auf einer Nachrichtenvorlage, die das Format und den Inhalt von E-Mail-Benachrichtigungen einschließlich des Nachrichtenbetreffs und Nachrichtentexts festlegt. Eine Vorlage ist ein Dokument im HTML-Format, das Sie anzeigen und bei Bedarf ändern können, um Benachrichtigungsmeldungen anzupassen. Der Vorlagentext kann dynamischen Inhalt umfassen, der bei Laufzeit durch Abfrage von Informationen aus der ausgeführten Instanz des Arbeitsablaufprozesses generiert wird. Sie haben die Möglichkeit, einen Bericht über die Ergebnisse der Ausführung des Arbeitsablaufs als Anlage zur Benachrichtigungsmeldung beizufügen.

Web-Interface-Adresse

Mit der Einstellung „Web-Interface-Adresse" wird die Adresse (URL) des Quest One ActiveRoles-Web-Interface angegeben. Diese Einstellung wird von der Aktivität verwendet, um Hyperlinks in den Benachrichtigungsmeldungen zu erstellen.

E-Mail-Server

Mit der Einstellung „E-Mail-Server" werden der Name und andere Parameter des E-Mail-Servers angegeben, die zur Übermittlung von Benachrichtigungsmeldungen verwendet werden.

Skriptaktivität

Skriptaktivitäten werden üblicherweise verwendet, um automatisierte Schritte in einem Arbeitsablaufprozess durchzuführen. Eine Skriptaktivität wird durch ein in Quest One ActiveRoles erstelltes Skriptmodul definiert. Jedes Skriptmodul enthält einen Skriptcode, der bestimmte Funktionen implementiert. Neue Skriptmodule können frei hinzugefügt werden, und das in einem Skriptmodul enthaltene Skript kann bei Bedarf weiterentwickelt und überprüft werden. So können benutzerdefinierte Funktionen erstellt werden. Dies bietet die Möglichkeit, die von einem Arbeitsablauf durchgeführten Vorgänge zu erweitern.

Die Skriptaktivität hat die folgenden grundlegenden Konfigurationseinstellungen:

- **Zu verwendendes Skript.** Gibt das Skriptmodul an, das von der Aktivität verwendet werden soll. Normalerweise implementiert das im Skriptmodul vorhandene Skript mindestens zwei Funktionen: die Funktion, die von der Aktivität ausgeführt wird, und die Funktion, die die Aktivitätsparameter definiert.
- **Auszuführende Funktion.** Gibt die Skriptfunktion an, die von der Aktivität ausgeführt wird.
- **Funktion zur Deklaration der Parameter.** Gibt die Skriptfunktion an, die die Aktivitätsparameter definiert. Für jeden Parameter definiert diese Funktion den Namen des Parameters und andere Merkmale wie etwa eine Beschreibung, eine Liste der möglichen Werte, den Standardwert und ob ein Wert erforderlich ist. Normalerweise werden die Parameter von der Funktion namens „onInit" deklariert.
- **Parameterwerte.** Wenn Quest One ActiveRoles eine Skriptaktivität ausführt, gibt es die Parameterwerte an die von dieser Aktivität ausgeführte Skriptfunktion weiter. Die von der Aktivität durchgeführten Vorgänge und die Ergebnisse dieser Vorgänge hängen von den Parameterwerten ab.

Weitere Informationen und Anweisungen, die sich auf den Entwurf, die Implementierung und die Verwendung von Skripts, Skriptmodulen und Skriptaktivitäten beziehen, finden Sie in der ActiveRoles SDK.

Benachrichtigung

Sie können eine Skriptaktivität darauf konfigurieren, Empfänger als Abonnenten der Benachrichtigungen folgender Ereignisse festzulegen:

- **Aktivität erfolgreich abgeschlossen.** Wenn diese Aktivität so konfiguriert wurde, dass Benachrichtigungen über dieses Ereignis erfolgen, versendet ActiveRoles eine Benachrichtigungs-E-Mail, wenn während der Ausführung dieser Aktivität keine erheblichen Fehler festgestellt wurden.

- **Aktivität hat einen Fehler festgestellt.** Wenn diese Aktivität so konfiguriert wurde, dass Benachrichtigungen über dieses Ereignis erfolgen, versendet ActiveRoles eine Benachrichtigungs-E-Mail, wenn während der Ausführung dieser Aktivität erhebliche Fehler festgestellt wurden.

Die Benachrichtigungseinstellungen geben das Ereignis an, über das eine Benachrichtigung versendet werden soll, sowie die Empfänger der Benachrichtigung. Wenn sie vom Arbeitsablauf ausgeführt wird, verfasst diese Aktivität eine dem angegebenen Ereignis entsprechende Benachrichtigung. ActiveRoles hält die von der Aktivität vorbereitete Meldung zurück und sendet die Meldung bei Eintritt des Ereignisses an die angegebenen Empfänger. Die Benachrichtigungseinstellungen sind vergleichbar mit den Benachrichtigungseinstellungen einer Benachrichtigungsaktivität (siehe Abschnitt Benachrichtigungsaktivität weiter oben in diesem Dokument).

Fehlerbehebung

Bei der Konfiguration einer Skriptaktivität können Sie wählen, ob von dieser Aktivität festgestellte Fehler unterdrückt werden sollen. Die folgende Option ist verfügbar: **Arbeitsablauf fortsetzen, auch wenn bei dieser Aktivität ein Fehler festgestellt wird** Wenn diese Option nicht ausgewählt ist (Standardeinstellung), führt eine von der Aktivität festgestellte Fehlerbedingung dazu, dass ActiveRoles den Arbeitsablauf beendet. Wenn Sie diese Option auswählen, wird der Arbeitsablauf unabhängig davon fortgesetzt, ob die Aktivität eine Fehlerbedingung feststellt oder nicht.

Wenn-Dann-Genehmigungsaktivität

Eine Wenn-Dann-Sonst-Aktivität wird verwendet, um einen von zwei oder mehr alternativen Zweigen abhängig von den für die Zweige definierten Bedingungen auszuführen. Sie enthält eine geordnete Reihe von Zweigen und führt den ersten Zweig aus, dessen Bedingung TRUE ist. Sie können so viele Zweige wie Sie möchten zu einer Wenn-Dann-Sonst-Aktivität hinzufügen, und Sie können auch so viele Aktivitäten wie Sie möchten zu jedem Zweig hinzufügen.

Für jeden Zweig einer Wenn-Dann-Sonst-Aktivität kann eine individuelle Bedingung festgelegt werden. Wenn eine Wenn-Dann-Sonst-Aktivität startet, prüft sie, ob die für ihren ersten (äußersten linken) Zweig festgelegte Bedingung wahr ist. Wenn die Bedingung erfüllt ist, werden die im Zweig enthaltenen Aktivitäten ausgeführt; andernfalls wird geprüft, ob die für den nächsten Zweig (von links nach rechts) festgelegte Bedingung wahr ist, etc.

Beachten Sie bei der Konfiguration von Wenn-Dann-Sonst-Zweigbedingungen folgende Hinweise:

- Nur der erste Zweig, dessen Bedingung TRUE ergibt, wird ausgeführt.
- Eine Wenn-Dann-Sonst-Aktivität kann beendet werden, ohne dass irgendeine ihrer Zweige ausgeführt wurde, wenn sich die für jeden Zweig festgelegte Bedingung als FALSE erweist.

Wenn keine Bedingung für einen Zweig definiert ist, so wird der Zweig so behandelt, als wenn eine permanent TRUE Bedingung vorliegt. Daher sollte der letzte (äußerst rechte) Zweig normalerweise über keine Bedingung verfügen, d.h. der Zweig sollte immer TRUE ergeben. Auf diese Weise fungiert der letzte Zweig als der „Sonst"-Zweig, der ausgeführt wird, wenn die Bedingungen für die anderen Zweige nicht erfüllt sind. Es ist ratsam, eine Bedingung für jeden Zweig in einer Wenn-Dann-Sonst-Aktivität mit Ausnahme des letzten Zweigs zu definieren, um zu gewährleisten, dass die Aktivität immer einen bestimmten Zweig ausführt.

Wenn-Dann-Zweigbedingungen

Eine Wenn-Dann-Aktivität ist darauf ausgelegt, genau einen Zweig der Aktivität aus einer Reihe von Zweigen auszuwählen. Bei jedem Zweig überprüft die Aktivität die Zweigbedingungen und führt den ersten jener Zweige aus, dessen Bedingung zu WAHR ausgewertet wird.

Bei der Konfiguration eines Wenn-Dann-Zweigs müssen Sie mindestens eine Bedingung hinzufügen, sind aber in der Anzahl der Bedingungen, die Sie für einen Zweig hinzufügen können, nicht eingeschränkt. Sie können mit Hilfe verschiedener Operatoren Bedingungen hinzufügen, löschen und gruppieren. Es ist möglich, Bedingungsgruppen in anderen Bedingungsgruppen zu verschachteln, um die gewünschten Ergebnisse zu erreichen.

Eine Bedingungsgruppe enthält eine oder mehrere Bedingungen, die durch denselben logischen Operator miteinander verbunden sind. Durch die Gruppierung von Bedingungen geben Sie an, dass diese Bedingungen als eine Einheit bewertet werden sollen. Der Effekt ist derselbe, als wenn Sie einen Ausdruck in einer mathematischen Gleichung oder in einer logischen Aussage in Klammern setzen.

Standardmäßig wird eine einzelne, implizite Bedingungsgruppe erstellt, wenn Sie eine Zweigbedingung hinzufügen. Sie können weitere Bedingungsgruppen erstellen, um eine Reihe von Bedingungen zu gruppieren und um gruppierte Bedingungen innerhalb anderer Bedingungsgruppen zu verschachteln.

In einer Bedingungsgruppe sind die Bedingungen über die logischen Operatoren AND, OR, NOT AND oder NOT OR miteinander verknüpft:

- Die AND-Gruppe ergibt TRUE (wahr), wenn alle Bedingungen in der Gruppe TRUE (wahr) sind.
- Die ODER Gruppe ergibt TRUE (wahr), wenn eine der Bedingungen in der Gruppe TRUE (wahr) ist.
- Die Gruppe NOT AND ergibt TRUE (wahr), wenn eine der Bedingungen in der Gruppe FALSE (falsch) ergibt.
- Die Gruppe NOT OR ergibt TRUE (wahr), wenn alle Bedingungen in der Gruppe FALSE (falsch) ergeben.

Standardmäßig ist AND der logische Operator zwischen den Bedingungen in einer Bedingungsgruppe. Es ist möglich, den logischen Operator zu ändern, indem die Bedingungsgruppe in einen anderen Gruppentyp umgewandelt wird.

Wenn Sie eine Bedingung hinzufügen, fordert Sie der Workflow Designer zunächst zur Angabe auf, was die Bedingung bewerten soll. Die folgenden Optionen sind verfügbar:

- **Eigenschaft des Arbeitsablaufinitiators.** Diese Option dient dazu, den Wert einer bestimmten Eigenschaft des Benutzers zu bewerten, dessen Anfrage den Arbeitsablauf gestartet hat. Sie können die gewünschte Eigenschaft auswählen, wenn Sie eine Bedingung konfigurieren.
- **Ausführungsstatus der Aktivität.** Diese Option ist darauf ausgelegt, auszuwerten, ob ActiveRoles bei der Ausführung einer bestimmten Aktivität einen Fehler festgestellt hat. Sie können die gewünschte Aktivität bei der Konfiguration einer Bedingung auswählen. Beachten Sie, dass Aktivitäten bei Auswahl dieser Option so konfiguriert sein müssen, dass der Arbeitsablauf auch dann fortgesetzt werden kann, wenn bei einer Aktivität ein Fehler auftritt (Hinweise zu den CRUD-Aktivitäten finden Sie im Abschnitt Fehlerbehebung).
- **Arbeitsablaufparamaterwert.** Diese Option dient zur Bewertung des Werts eines bestimmten Parameters des Arbeitsablaufs. Sie können den gewünschten Parameter bei der Konfiguration einer Bedingung auswählen.

- **Eigenschaft des Objektes aus dem Arbeitsablauf-Datenkontext.** Diese Option ist darauf ausgelegt, den Wert einer bestimmten Eigenschaft jenes Objekts auszuwerten, das von der Wenn-Dann-Aktivität auf Basis der zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefundenen Daten ausgewählt wird. Bei der Konfiguration einer Zweigbedingung können Sie die gewünschte Eigenschaft wählen und angeben, welches Objekt von der Aktivität nach Auswertung der Bedingung zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll.
- **Wert durch Regel-Ausdruck generiert.** Diese Option dient zur Bewertung des Zeichenkettenwerts einer bestimmten Regelausnahme. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. ActiveRoles errechnet den Wert Ihres Regel-Ausdrucks bei der Auswertung der Bedingung zum Ausführungszeitpunkt des Arbeitsablaufs.

In einem Änderungs-Arbeitslauf stehen zusätzlich zu den obenstehenden Optionen folgende Optionen zur Verfügung:

- **Eigenschaft des Arbeitsablaufzielobjekts.** Diese Option dient dazu, den Wert einer bestimmten Eigenschaft des Zielobjekts der Anfrage zu bewerten, die den Arbeitsablauf gestartet hat. Sie können die gewünschte Eigenschaft auswählen, wenn Sie eine Bedingung konfigurieren.
- **Geänderter Wert der Eigenschaft des Arbeitsablaufzielobjekts.** Diese Option dient dazu, den Wert zu bewerten, dessen Zuweisung zu einer bestimmten Eigenschaft des Arbeitsablaufzielobjekts angefordert wurde, das die angeforderte Änderung an der Eigenschaft des Zielobjekts der Anfrage darstellt, die den Arbeitsablauf gestartet hat. Sie können die gewünschte Eigenschaft auswählen, wenn Sie eine Bedingung konfigurieren.
- **Gewählte Aktion genehmigen.** Diese Option ist darauf ausgelegt, den Namen der von der genehmigenden Instanz verwendete Aktionsschaltfläche auszuwerten, um die Genehmigungsaufgabe abzuschließen, die von einer bestimmten Genehmigungsaktivität erstellt wurde. Verwenden Sie diese Option, um festzulegen, welche Aktionsschaltfläche die genehmigende Instanz verwendet hat, um den genehmigungspflichtigen Vorgang zuzulassen. Sie können die gewünschte Genehmigungsaktivität bei der Konfiguration einer Bedingung auswählen.

Wenn Sie die Einheit oder das Feld angegeben haben, die bzw. das die Bedingung bewerten soll, dann können Sie einen Vergleichsoperator auswählen und einen Vergleichswert angeben. Die Liste der Optionen, die zur Angabe eines Vergleichswertes zur Verfügung stehen, hängt von der Einheit oder dem Feld ab, auf deren bzw. dessen Auswertung die Bedingung konfiguriert wurde. In der folgenden Tabelle werden die Vergleichswertoptionen zusammengefasst.

AUSZUWERTENDE BEDINGUNG	VERGLEICHSWERTOPTIONEN
Eigenschaft des Arbeitsablaufzielobjekts – ODER – Eigenschaft des Arbeitsablaufinitiators – ODER – Geänderter Wert der Eigenschaft des Arbeitsablaufzielobjekts – ODER – Arbeitsablaufparameterwert – ODER – Eigenschaft des Objekts aus dem Arbeitsablaufdatenkontext – ODER – Durch Regel-Ausdruck generierter Wert	• Textzeichenfolge • Eigenschaft des Arbeitsablaufzielobjekts • Eigenschaft des Arbeitsablaufinitiators • Geänderter Wert der Eigenschaft des Arbeitsablaufzielobjekts • Arbeitsablaufparameterwert • Eigenschaft des Objekts aus dem Arbeitsablaufdatenkontext • Durch Regel-Ausdruck generierter Wert
Ausführungsstatus der Aktivität	• Nicht ausgeführt • Erfolgreich abgeschlossen • Einen Fehler festgestellt
Gewählte Aktion genehmigen	• Der Name einer Aktionsschaltfläche • Vom Skript generierter Wert

Eine Kurzbeschreibung der Vergleichsoperatoren und Vergleichswertoptionen finden Sie unter Suchfilter.

Fehlerbehebung

Bei der Konfiguration einer Wenn-Dann-Aktivität können Sie wählen, ob von dieser Aktivität festgestellte Fehler unterdrückt werden sollen. Die folgende Option ist verfügbar: **Arbeitsablauf fortsetzen, auch wenn bei dieser Aktivität ein Fehler festgestellt wird** Wenn diese Option nicht ausgewählt ist (Standardeinstellung), führt eine von der Aktivität festgestellte Fehlerbedingung dazu, dass ActiveRoles den Arbeitsablauf beendet. Wenn Sie diese Option auswählen, wird der Arbeitsablauf unabhängig davon fortgesetzt, ob die Wenn-Dann-Aktivität oder eine in der Wenn-Dann-Aktivität enthaltene Aktivität eine Fehlerbedingung feststellt oder nicht.

Aktivität stoppen/unterbrechen

Eine Stoppen/Unterbrechen-Aktivität wird verwendet, um sofort alle Aktivitäten einer laufenden Arbeitsablaufinstanz zu beenden. Sie können sie innerhalb eines Zweigs einer Wenn-Dann-Sonst-Aktivität verwenden, um den Arbeitsablauf zu beenden, wenn eine bestimmte Bedingung eintritt.

Als Beispiel dient eine Anforderung für die Bestätigung der angeforderten Datenänderungen, um bestimmte Vorgänge zu verweigern, weil die Anwendung solcher Vorgänge dazu führen würde, dass inakzeptable Daten in das Verzeichnis geschrieben werden. Um diese Anforderung zu erfüllen, können Sie einen Arbeitsablauf mit einem Wenn-Dann-Sonst-Zweig verwenden, der bei Erkennung inakzeptabler Daten im angeforderten Vorgang ausgeführt wird, und dann eine Stoppen/Unterbrechen-Aktivität zu diesem Zweig hinzufügen. Auf diese Weise sperrt Ihr Arbeitsablauf die unerwünschten Vorgänge und schützt so die Verzeichnisdaten.

Die Stoppen/Unterbrechen-Aktivität schreibt eine Nachricht ins Protokoll, wenn sie die Arbeitsablaufinstanz beendet. Sie können einen Nachrichtentext als eine Aktivitätseinstellung festlegen, um den Grund für die Beendigung der Arbeitsablaufinstanz anzugeben. Die Aktivität umfasst diese Nachricht in dem Ereignis, das in das Ereignisprotokoll des „EDM-Server"-Ereignisprotokolls auf dem Computer geschrieben wird, auf dem der ActiveRoles-Verwaltungsdienst ausgeführt wird.

Aktivität „Berichtsabschnitt hinzufügen"

Sie können die Aktivität „Berichtsabschnitt hinzufügen" verwenden, um benutzerdefinierte Informationen zum Bericht über den Änderungsverlauf (falls der Arbeitsablauf durch eine Vorgangsanforderung gestartet wurde) oder den Ausführungsverlaufsbericht (im Falle eines Automatisierungs-Arbeitsablaufs) hinzufügen. Die Aktivität fügt einen separaten Abschnitt zum Bereich **Arbeitsablaufaktivitäten und Richtlinienaktionen** des Berichts hinzu. Der Abschnitt besteht aus einem Kopf- und Textteil. Die Aktivität stellt folgende Optionen zur Konfiguration des im Kopf- und Textteil des Berichtsabschnitts anzuzeigenden Texts zur Verfügung:

- Sie können festlegen, ob der Berichtsabschnitt Informationen zu einem erfolgreichen Vorgang oder zu einer Fehlerbedingung anzeigen soll. In letzterem Falle wird der Text im Kopf- und Textteil des Berichtsabschnitts in roter Farbe angezeigt.
- Sie können den Kopftext aus Dateneinträgen zusammenstellen lassen, die bei der Ausführung der Aktivität errechnet werden. Die Aktivität bietet verschiedene Dateneingabetypen und ermöglicht es, im Kopftext die Eigenschaften am Arbeitsablauf beteiligter und verwandter Objekte, Datum und Uhrzeit der Aktivitätsausführung sowie Arbeitsablauf-Parameter einzuschließen.
- Sie können den Textteil darauf konfigurieren, mehrere Zeichenfolgen einzuschließen, wobei jede Zeichenfolge durch die gleichen Optionen erstellt wird, die auch für den Kopftext verfügbar sind. Somit kann der Textteil zusätzlich zu Literalzeichenfolgen und Formatierungszeichen auch Informationen zu Objekteigenschaften und anderen Zeichenfolgewerten enthalten, die von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs errechnet werden.

Sie können die Aktivität „Berichtsabschnitt hinzufügen" auch zu einer bestimmten Wenn-Dann-Verzweigung hinzufügen, damit im Bericht angezeigt wird, dass beim Arbeitsablauf der betreffende Aktivitätenzweig ausgeführt wurde.

Suchaktivität

Mit Hilfe einer Suchaktivität können Sie Verzeichnisdaten nach Objekten, etwa nach Benutzern oder Gruppen, durchsuchen, die mit den Kriterien übereinstimmen, die Sie auf Basis der Objekteigenschaften, Objektspeicherorte und anderer in der Ausführungsumgebung des Arbeitsablaufs verfügbarer Informationen festlegen, und diese Objekte an andere Aktivitäten weiterleiten, damit der Arbeitsablauf die notwendigen Aktionen auch an diesen durchführen kann. Sie können Aktivitäten in eine Suchaktivität einfügen und von diesen Aktivitäten die von der Suchaktivität gefundenen Objekte verarbeiten lassen.

Die folgenden Themen behandeln die konfigurierbaren Einstellungen einer Suchaktivität.

- Suchszenario
- Objekttyp
- Suchbereich
- Suchoptionen
- Suche nach inaktiven Konten
- Suchfilter
- Benachrichtigung
- Fehlerbehebung
- „Ausführen als"-Optionen
- Zusätzliche Einstellungen
- Suchaktivität beenden

Suchszenario

Sie können eine Suchaktivität für folgende Vorgänge konfigurieren:

- **In der Organisationseinheit oder im Container suchen.** Sucht innerhalb einer bestimmten Organisationseinheit oder eines bestimmten Containers nach Objekten, die Ihre Suchkriterien erfüllen.
- **Nach vom Benutzer oder von der Gruppe verwaltete oder in ihrem Besitz befindlichen Ressourcen suchen.** Sucht nach den verwalteten Objekten eines bestimmten Benutzers oder einer bestimmten Gruppe, die Ihre Suchkriterien erfüllen. Verwaltete Objekte eines Benutzers oder einer Gruppe sind jene Objekte, für die der Benutzer oder die Gruppe als primärer oder sekundärer Besitzer festgelegt ist.
- **In der Gruppe nach ihren Mitgliedern suchen.** Sucht nach den Mitgliedern einer bestimmten Gruppe, die Ihre Suchkriterien erfüllen.
- **Nach direkten Berichten des Benutzers suchen.** Sucht nach den direkten Berichten eines bestimmten Benutzers, die Ihre Suchkriterien erfüllen. Mit den Benutzern direkter Berichte sind jene Benutzer gemeint, für die dieser Benutzer der Verwalter ist.
- **Suche innerhalb der Objektattribute (ASQ-Suche).** Nach Objekten suchen, die in einem bestimmten Attribut eines Objektes aufgelistet sind, die mit den Suchkriterien übereinstimmen.

Objekttyp

Sie können den Typ der Objekte angeben, nach denen die Aktivität suchen sollen. Die Liste, aus der Sie den Objekttyp wählen, hängt vom gewählten Suchszenario ab.

SUCHSZENARIO	ZU SUCHENDE OBJEKTTYPEN
In der Organisationseinheit oder im Container suchen	• Benutzer • Kontakte • Gruppen • Computer • Drucker • Organisationseinheiten • Freigegebene Ordner • Exchange-Empfänger • Inaktive Konten • Alle Objekte
Nach vom Benutzer oder von der Gruppe verwaltete oder in ihrem Besitz befindlichen Ressourcen suchen – ODER – **Suche innerhalb der Objektattribute (ASQ-Suche)**	• Benutzer • Kontakte • Gruppen • Computer • Drucker • Organisationseinheiten • Freigegebene Ordner • Exchange-Empfänger • Alle Objekte
In der Gruppe nach ihren Mitgliedern suchen	• Benutzer • Kontakte • Gruppen • Computer • Exchange-Empfänger • Alle Objekte
Nach direkt Unterstellten des Benutzers suchen	• Benutzer • Alle Objekte

Suchbereich

Der Suchbereich legt fest, wo nach den Objekten des angegebenen Typs gesucht werden soll. Die Suchbereichseinstellungen sind abhängig vom jeweiligen Suchszenario und lauten wie folgt:

SUCHSZENARIO	VERFÜGBARE SUCHBEREICHSEINSTELLUNGEN
In der Organisationseinheit oder im Container suchen	• **Fester Container in Verzeichnis.** Sucht in der jeweiligen Organisationseinheit bzw. im jeweiligen Container. Sie können die gewünschte Organisationseinheit bzw. den Container in Active Directory bei der Konfiguration einer Suchaktivität wählen. • **Übergeordnete Organisationseinheit des Arbeitsablaufzielobjekts.** Sucht in der Organisationseinheit, welche das Zielobjekt der Anforderung enthält, die den Arbeitsablauf gestartet hat. • **Vom Arbeitsablaufparameter erkanntes Objekt.** Sucht in der Organisationseinheit oder im Container, die bzw. der durch den Wert eines bestimmten Arbeitsablaufparameters angegeben wurde. Sie können den gewünschten Parameter bei der Konfiguration einer Suchaktivität auswählen. • **Objektes aus Arbeitsablauf-Datenkontext.** Sucht in der Organisationseinheit oder im Container, die bzw. der von der Suchaktivität auf Basis der zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefundenen Daten ausgewählt wird. Bei der Konfiguration einer Suchaktivität können Sie angeben, welche Organisationseinheit bzw. welcher Container von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll. • **Durch Regel-Ausdruck des DN-Werts identifiziertes Objekt.** Sucht in der Organisationseinheit oder im Container, deren bzw. dessen eindeutiger Name (Distinguished Name, DN) vom Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben wird. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration einer Suchaktivität erstellen.
Nach vom Benutzer oder von der Gruppe verwaltete oder in ihrem Besitz befindlichen Ressourcen suchen	• **Arbeitsablaufzielobjekt.** Sucht nach Ressourcen, die vom Zielobjekt der Anforderung, die den Arbeitsablauf gestartet hat, verwaltet bzw. besessen werden. • **Vom Arbeitsablaufparameter erkanntes Objekt.** Sucht nach Ressourcen, die vom Objekt verwaltet oder besessen werden, welches durch den Wert eines bestimmten Arbeitsablaufsparameters angegeben wurde. Sie können den gewünschten Parameter bei der Konfiguration einer Suchaktivität auswählen. • **Objekt aus Arbeitsablauf-Datenkontext.** Sucht nach Ressourcen, die vom Objekt verwaltet oder besessen werden, welches durch die Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt wird. Bei der Konfiguration einer Suchaktivität können Sie angeben, welches Objekt von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll. • **Durch Regel-Ausdruck des DN-Werts identifiziertes Objekt.** Sucht nach Ressourcen, die vom Objekt verwaltet oder besessen werden, dessen eindeutiger Name (Distinguished Name, DN) vom Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben wird. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration einer Suchaktivität erstellen.

SUCHSZENARIO	VERFÜGBARE SUCHBEREICHSEINSTELLUNGEN
In der Gruppe nach ihren Mitgliedern suchen	• **Arbeitsablaufzielobjekt.** Sucht nach Mitgliedern der Gruppe, die das Zielobjekt der Anforderung ist, die den Arbeitsablauf gestartet hat. • **Vom Arbeitsablaufparameter erkanntes Objekt.** Sucht in der Gruppe, die vom Wert eines bestimmten Arbeitsablaufparameters angegeben wird. Sie können den gewünschten Parameter bei der Konfiguration einer Suchaktivität auswählen. • **Objekt aus Arbeitsablauf-Datenkontext.** Sucht nach Mitgliedern des Gruppenobjekts, welches durch die Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt wird. Bei der Konfiguration einer Suchaktivität können Sie angeben, welches Gruppenobjekt von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll. • **Durch Regel-Ausdruck des DN-Werts identifiziertes Objekt.** Sucht in der Gruppen, deren eindeutiger Name (Distinguished Name, DN) vom Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben wird. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration einer Suchaktivität erstellen.
Nach direkt Unterstellten des Benutzers suchen	• **Arbeitsablaufzielobjekt.** Sucht nach direkten Berichten des Zielobjekts der Anforderung, die den Arbeitsablauf gestartet hat. • **Vom Arbeitsablaufparameter erkanntes Objekt.** Sucht nach direkten Berichten des Objekts welches durch den Wert eines bestimmten Arbeitsablaufsparameters angegeben wurde. Sie können den gewünschten Parameter bei der Konfiguration einer Suchaktivität auswählen. • **Objekt aus Arbeitsablauf-Datenkontext.** Sucht nach direkten Berichten des Objekts, welches durch die Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt wird. Bei der Konfiguration einer Suchaktivität können Sie angeben, welches Objekt von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll. • **Durch Regel-Ausdruck des DN-Werts identifiziertes Objekt.** Sucht nach direkten Berichten des Objekts, dessen eindeutiger Name (Distinguished Name, DN) vom Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben wird. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration einer Suchaktivität erstellen.
Suche innerhalb der Objektattribute (ASQ-Suche)	• **Festes Objekt im Verzeichnis.** Sucht innerhalb eines bestimmten Attributs des angegebenen Objekts. Sie können das gewünschte Objekt in Active Directory bei der Konfiguration einer Suchaktivität wählen. • **Arbeitsablaufzielobjekt.** Sucht innerhalb eines bestimmten Attributs des Zielobjekts der Anforderung, die den Arbeitsablauf gestartet hat. • **Objekt aus Arbeitsablauf-Datenkontext.** Sucht innerhalb eines bestimmten Attributs des Objekts, welches durch die Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt wird. Bei der Konfiguration einer Suchaktivität können Sie angeben, welches Objekt von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll.

Suchoptionen

Die Aktivität stellt verschiedene Optionen zur Verfügung, mit denen Sie Ihre Suche verfeinern können. Welche Optionen zur Verfügung stehen, hängt vom Suchszenario und dem zu suchenden Objekttyp ab, entsprechend der untenstehenden Tabellen.

In der folgenden Tabelle werden die suchszenariospezifischen Suchoptionen zusammengefasst.

SUCHSZENARIO	VERFÜGBARE SUCHOPTIONEN
In der Organisationseinheit oder im Container suchen	• **Nur direkt untergeordnete Objekte der Organisationseinheit oder des Containers abrufen.** Verwenden Sie diese Option, um die Suche auf Objekte einzuschränken, die in Active Directory der angegebenen Organisationseinheit bzw. dem angegebenen Container direkt untergeordnet sind • **Jedes beliebige Objekt aus der Organisationseinheit oder dem Container abrufen.** Verwenden Sie diese Option, um in der gesamten Verzeichnisstruktur zu suchen, deren Wurzel die angegebene Organisationseinheit bzw. der angegebene Container ist.
Nach vom Benutzer oder von der Gruppe verwaltete oder in ihrem Besitz befindlichen Ressourcen suchen	• **Vom Benutzer oder der Gruppe (primärer Besitzer) verwaltete Objekte abrufen.** Verwenden Sie diese Option, um nach Objekten zu suchen, bei denen der jeweilige Benutzer bzw. die jeweilige Gruppe in der Eigenschaft „Verwaltet von" angegeben ist. • **Objekte abrufen, bei welchen der Benutzer oder die Gruppe ein sekundärer Besitzer ist.** Verwenden Sie diese Option, um nach Objekten zu suchen, bei denen der jeweilige Benutzer bzw. die jeweilige Gruppe in der Eigenschaft „Sekundäre Besitzer" angegeben ist. • **Aufgrund der Mitgliedschaft in Gruppen (indirekte Besitzerschaft) verwaltete oder im Besitz befindliche Objekte abrufen.** Verwenden Sie diese Option, um nach Objekten zu suchen, bei denen der jeweilige Benutzer bzw. die jeweilige Gruppe ein direktes oder indirektes Mitglied der Gruppe ist, die in der Eigenschaft „Verwaltet von" oder „Sekundäre Besitzer" angegeben ist.
In der Gruppe nach ihren Mitgliedern suchen	• **Auch indirekte Mitglieder abrufen.** Verwenden Sie diese Option, um in Ihren Suchergebnissen indirekte Mitglieder der jeweiligen Gruppe einzuschließen. Mit dieser Option sucht die Aktivität nicht nur nach Objekte, die direkt zur Gruppe hinzugefügt wurden (direkte Mitglieder), sondern auch nach indirekten Mitgliedern - Objekte, die aufgrund ihrer Mitgliedschaft in anderen Gruppen, die direkte oder indirekte Mitglieder der jeweiligen Gruppe sind, zur Gruppe gehören. • **Auch ausstehende Mitglieder abrufen.** Verwenden Sie diese Option, um in Ihren Suchergebnissen Objekte einzuschließen, für die das Hinzufügen zur Gruppe mit Hilfe der Funktion „Temporäre Gruppenmitgliedschaften" von ActiveRoles geplant ist.
Suche innerhalb der Objektattribute (ASQ-Suche)	• **Mit diesem Attribut suchen.** Gibt das Attribut für die ASQ-Suche an. Dies muss ein Attribut sein, das eindeutige Namen (Distinguished Names) speichert, wie etwa das Attribut „Mitglied von" oder „Verwaltet von". Die Suche wird unter den Objekten durchgeführt, die durch die im Attribut gefundenen eindeutigen Namen gekennzeichnet sind. Zum Beispiel sucht eine Suche innerhalb des Attributs „Mitglied von" eines Benutzerkontos nach Gruppen, in denen der Benutzer Mitglied ist.

In der folgenden Tabelle werden die für den Objekttyp spezifischen Suchoptionen aufgeführt. Die Suchergebnisse erhalten nur die Objekte, die den von Ihnen gewählten Optionen entsprechen.

ZU SUCHENDE OBJEKTE	VERFÜGBARE SUCHOPTIONEN
Benutzer	• **Benutzer mit Exchange-Postfach.** Sucht nach Benutzern, die über ein Microsoft Exchange-Postfach verfügen. • **Benutzer mit externen E-Mail-Adressen.** Sucht nach Benutzern, die über ein externes Microsoft Exchange-fähiges Postfach verfügen. • **Inaktive Benutzerkonten.** Sucht nach Benutzerkonten, die seit einer bestimmten Anzahl von Tagen nicht mehr zur Anmeldung verwendet wurden, über ein Kennwort verfügen, das älter als eine bestimmte Anzahl von Tagen ist, oder die länger als eine bestimmte Anzahl von Tagen abgelaufen sind.
Kontakte	• **Kontakte mit externen E-Mail-Adressen.** Sucht nach Benutzern, die über ein externes Microsoft Exchange-fähiges Postfach verfügen.
Gruppen	• **Mail-aktivierte Gruppen.** Sucht nach Microsoft Exchange-fähigen Gruppen (Verteilerlisten). • **Sicherheit.** Sucht nach Sicherheitsgruppen. • **Verteilung.** Sucht nach Verteilungsgruppen. • **Lokale Domäne.** Sucht nach Gruppen der lokalen Domäne. • **Global.** Sucht nach globalen Gruppen. • **Universell.** Sucht nach universellen Gruppen. • **Dynamische Gruppe.** Sucht nach Gruppen, die in Quest One ActiveRoles als dynamische Gruppen konfiguriert sind. • **Gruppenfamilie.** Sucht nach Gruppen, die Gruppenfamilien-Konfigurationen für Quest One ActiveRoles speichern (Gruppenfamilien-Konfigurationsspeichergruppen). • **Von der Gruppenfamilie kontrolliert.** Sucht nach Gruppen, die in Quest One ActiveRoles.von Gruppenfamilien-Regeln kontrolliert werden. • **Leer.** Sucht nach Gruppen, die keine Mitglieder enthalten. • **Deprovisioniert.** Sucht nach Gruppen, die mit Hilfe von Quest One ActiveRoles deprovisioniert wurden.
Computer	• **Rolle des Computers.** Sucht nach Computern in einer bestimmten Rolle. Sie können die Suche auf Workstations und Server oder auf Domänencontroller einschränken. • **Inaktive Computerkonten.** Sucht nach Computerkonten, die seit einer bestimmten Anzahl von Tagen nicht mehr zur Anmeldung verwendet wurden, über ein Kennwort verfügen, das älter als eine bestimmte Anzahl von Tagen ist, oder die länger als eine bestimmte Anzahl von Tagen abgelaufen sind.
Drucker	• **Druckerfunktionen.** Sucht nach Druckern mit bestimmten Funktionen oder Merkmalen, wie etwa Druckermodell, Papierformat, Druckauflösung, Druckgeschwindigkeit und andere Fähigkeiten, einschließlich der Fähigkeit für doppelseitigen Druck, der Fähigkeit für mehrfarbigen Druck und der Fähigkeit zum Heften.

ZU SUCHENDE OBJEKTE	VERFÜGBARE SUCHOPTIONEN
Exchange-Empfänger	• **Benutzer mit Exchange-Postfach.** Sucht nach Benutzern, die über ein Microsoft Exchange-Postfach verfügen. • **Benutzer mit externen E-Mail-Adressen.** Sucht nach Benutzern, die über ein externes Microsoft Exchange-fähiges Postfach verfügen. • **Mail-aktivierte Gruppen.** Sucht nach Microsoft Exchange-fähigen Gruppen (Verteilerlisten). • **Kontakte mit externen E-Mail-Adressen.** Sucht nach Benutzern, die über ein externes Microsoft Exchange-fähiges Postfach verfügen. • **Mail-aktivierte öffentliche Ordner.** Sucht nach Microsoft Exchange Mail-aktivierten öffentlichen Ordnern. • **Abfragebasierte Verteilergruppen.** Sucht nach Microsoft Exchange-abfragebasierten Verteilergruppen. • **Raumpostfächer.** Sucht nach Benutzerkonten, die Microsoft Exchange-Raumpostfächer darstellen. • **Gerätepostfächer.** Sucht nach Benutzerkonten, die Microsoft Exchange-Gerätepostfächer darstellen. • **Verknüpfte Postfächer.** Sucht nach Benutzerkonten, die verknüpfte Microsoft Exchange-Postfächer darstellen. • **Gemeinsam genutzte Postfächer.** Sucht nach Benutzerkonten, die gemeinsam genutzte Microsoft Exchange-Postfächer darstellen. • **Postfächer auf diesem Server.** Sucht nach Benutzerkonten, die Microsoft Exchange-Postfächer darstellen, welche auf einem bestimmten Postfachserver gehostet sind. Sie können den gewünschten Postfachserver wählen. • **Postfächer in diesem Postfachspeicher oder in dieser Postfachdatenbank.** Sucht nach Benutzerkonten, die Microsoft Exchange-Postfächer darstellen, welche in einem bestimmten Postfachspeicher oder einer bestimmten Datenbank gespeichert sind. Sie können den gewünschten Postfachspeicher oder die gewünschte Datenbank wählen.
Inaktive Konten	• **Kontotyp.** Sucht nur nach Benutzerkonten, nur nach Computerkonten, oder sowohl nach Benutzer- wie auch nach Computerkonten. • **Inaktivitätskriterien.** Sucht nach Konten, die seit einer bestimmten Anzahl von Tagen nicht mehr zur Anmeldung verwendet wurden, über ein Kennwort verfügen, das älter als eine bestimmte Anzahl von Tagen ist, oder die länger als eine bestimmte Anzahl von Tagen vor dem aktuellen Datum abgelaufen sind.

Suche nach inaktiven Konten

Wenn Sie die Option **In der Organisationseinheit oder im Container suchen** wählen, können Sie die Aktivität darauf konfigurieren, nach inaktiven Benutzer- oder Computerkonten zu suchen. Der Objekttyp **Inaktive Konten** stellt die folgenden Suchoptionen zur Verfügung:

- **Zu suchender Kontotyp.** Sie können wählen, nur nach Benutzerkonten, nur nach Computerkonten oder sowohl nach Benutzer- wie auch nach Computerkonten zu suchen.
- **Nach Konten suchen, die seit einer bestimmten Anzahl von Tagen nicht mehr zur Anmeldung verwendet wurden.** Diese Option ermöglicht es Ihnen, den Zeitraum in Tagen anzugeben, für den ein Konto nicht zur Anmeldung verwendet wurde, und nach dem ein Konto als inaktiv gilt. Die Suche ruft ein bestimmtes Konto ab, wenn für dieses Konto länger als für die mit dieser Option angegebene Anzahl von Tagen keine erfolgreiche Anmeldung verzeichnet wurde.

Die Suchaktivität verwendet das Attribut „lastLogonTimeStamp" um den Zeitpunkt festzustellen, an dem ein bestimmter Benutzer oder Computer sich zuletzt erfolgreich angemeldet hat. Active Directory aktualisiert dieses Attribut nur periodisch und nicht jedes Mal, wenn sich ein Benutzer oder Computer anmeldet. Normalerweise beträgt die Aktualisierungsperiode 14 Tage. Das bedeutet, dass der Wert von „lastLogonTimeStamp" bis zu 14 Tage ungenau sein kann, der tatsächliche letzte Anmeldezeitpunkt ist also später als „lastLogonTimeStamp". Daher empfiehlt es sich, eine Anmeldungs-Inaktivitätsperiode von mehr als 14 Tagen zu wählen.

- **Nach Konten suchen, dessen Kennwort älter als eine bestimmte Anzahl von Tagen ist.** Diese Option ermöglicht es Ihnen, das Kennwortalter in Tagen anzugeben, nach dem ein Konto als inaktiv gilt. Die Suche ruft ein bestimmtes Konto ab, wenn das Kennwort des Kontos länger als für die mit dieser Option angegebene Anzahl von Tagen unverändert bleibt.
- **Nach Konten suchen, die länger als eine bestimmte Anzahl von Tagen vor dem aktuellen Datum abgelaufen sind.** Diese Option ermöglicht es Ihnen, die Anzahl von Tagen anzugeben, nach denen ein abgelaufenes Konto als inaktiv gilt. Die Suche ruft ein bestimmtes Konto ab, wenn das Konto über einen längeren Zeitraum in Tagen den Status „Inaktiv" besitzt, als mit dieser Option angegeben.

Die Option zur Suche nach inaktiven Konten ist ebenfalls verfügbar, wenn Sie die Aktivität darauf konfigurieren, nach dem Objekttyp **Benutzer** oder **Computer** zu suchen. Sie können die Suche auf inaktive Konten einschränken, indem Sie die geeigneten Optionen zur Definition inaktiver Konten verwenden. Diese Optionen sind die gleichen wie beim Objekttyp **Inaktive Konten**.

Suchfilter

Mit der Suchfilteroption können Sie Ihre Suche verfeinern, um Verzeichnisobjekte auf Basis der Objekteigenschaften (Attribute) ausfindig zu machen. So könnten Sie beispielsweise alle Teammitglieder einer bestimmten Abteilung finden wollen, die dem Verwalter namens „John Smith" unterstehen, oder vielleicht an Computerkonten interessiert sein, die für einen bestimmten Zeitraum nicht verwendet wurden. In beiden Fällen können Sie einen Suchfilter verwenden, um nach bestimmten Werten in den Objekteigenschaften zu suchen. So stellen Sie sicher, dass die Suchergebnisse nur die Objekte mit den gewünschten Eigenschaften enthalten.

Ein Suchfilter besteht aus Bedingungen, die mit „Und"- oder „Oder"-Logik kombiniert werden. Jede Bedingung stellt eine bestimmte Anweisung dar, welche die Kriterien angibt, mit denen die Aktivität feststellen soll, ob ein bestimmtes Objekt in den Suchergebnissen einzuschließen ist oder nicht. Zur Erstellung eines Filters müssen Sie mindestens eine Bedingung hinzufügen, aber Sie können so viele Bedingungen hinzufügen, wie Sie möchten. Durch die Verwendung mehrerer Bedingungen können Sie sehr komplexe Filter erstellen. Sie können mit Hilfe verschiedener Operatoren Filterbedingungen hinzufügen, löschen und gruppieren. Sie können sogar Bedingungsgruppen innerhalb von anderen Bedingungsgruppen verschachteln, um die gewünschten Resultate zu erhalten. Wenn die Aktivität ausgeführt wird, wird der Filter ausgewertet, um festzustellen, ob die von der Suche gefundenen Objekte die im Filter angegebenen Suchkriterien erfüllen. Wenn ein Objekt die Kriterien erfüllt, wird es den Suchergebnissen hinzugefügt. Ansonsten wird es herausgefiltert. Wenn Sie keinen Filter erstellen, werden alle von der Suche gefundenen Objekte in den Suchergebnissen eingeschlossen.

Eine Filterbedingung besteht aus drei Teilen: dem Namen einer bestimmten Eigenschaft, dem Vergleichsoperator und dem Wert, mit dem die Eigenschaft verglichen werden soll (Vergleichswert). Einige Operatoren benötigen keinen Vergleichswert. Bei der Erstellung einer Bedingung wählen Sie zunächst eine bestimmte Eigenschaft. Dann wählen Sie den gewünschten Vergleichsoperator und geben falls nötig den gewünschten Vergleichswert an. Die Liste, aus der Sie einen Vergleichsoperator wählen können, hängt von dem Eigenschaftstyp ab, für den Sie die Bedingung erstellen. Ob Sie einen Vergleichswert angeben müssen, hängt vom Vergleichsoperator ab. Die folgende Tabelle fasst die verfügbaren Vergleichsoperatoren und Vergleichswerte zusammen.

Sie können bei der Konfiguration einer Filterbedingung aus den folgenden Vergleichsoperatoren wählen:

VERGLEICHSOPERATOR	GIBT AN, DASS
gleich	der Eigenschaftswert des Objekts dem Vergleichswert entspricht.
ist nicht gleich	der Eigenschaftswert des Objekts nicht dem Vergleichswert entspricht.
größer oder gleich	der Eigenschaftswert des Objekts größer oder gleich dem Vergleichswert ist.
kleiner oder gleich	der Eigenschaftswert des Objekts kleiner oder gleich dem Vergleichswert ist.
enthält	der Eigenschaftswert des Objekts den vom Vergleichswert angegebenen Text enthält.
enthält nicht	der Eigenschaftswert des Objekts nicht den vom Vergleichswert angegebenen Text enthält.
beginnt mit	Der vom Vergleichswert angegebene Text am Anfang des Eigenschaftswerts des Objekts steht.
beginnt nicht mit	Der vom Vergleichswert angegebene Text nicht am Anfang des Eigenschaftswerts des Objekts steht.
endet mit	Der vom Vergleichswert angegebene Text am Ende des Eigenschaftswerts des Objekts steht.
endet nicht mit	Der vom Vergleichswert angegebene Text nicht am Ende des Eigenschaftswerts des Objekts steht.
ist leer	die Eigenschaft nicht am Objekt angegeben ist.
ist nicht leer	die Eigenschaft des Objekts über einen Nicht-Nullwert verfügt.
bitweise und	jeder Teil des Eigenschaftswerts des Objekts dem zugehörigen Teil des Vergleichswerts entspricht.
bitweise oder	ein beliebiger Teil des Eigenschaftswerts des Objekts dem zugehörigen Teil des Vergleichswerts entspricht.
entspricht regulärem Ausdruck	der Eigenschaftswert des Objekts einem bestimmten regulären Ausdruck entspricht. Dies erfordert, dass es sich beim Vergleichswert um eine Textzeichenfolge handelt, welche den gewünschten regulären Ausdruck enthält.

Sie können bei der Konfiguration einer Filterbedingung aus den folgenden Vergleichswerten wählen:

VERGLEICHSWERT	BESCHREIBUNG
Textzeichenfolge	Eine Literalzeichenkette. Sie können bei der Konfiguration einer Filterbedingung die gewünschte Zeichenfolge eingeben.
Eigenschaft des Arbeitsablaufzielobjekts	Der Wert einer bestimmten Eigenschaft des Zielobjekts der Anforderung, die den Arbeitsablauf gestartet hat. Sie können bei der Konfiguration einer Filterbedingung die gewünschte Eigenschaft wählen. Normalerweise sollte es sich hierbei um eine Eigenschaft in Form eines Zeichenfolgewerts handeln.
Eigenschaft des Arbeitsablaufinitiators	Der Wert einer bestimmten Eigenschaft des Benutzers, dessen Anforderung den Arbeitsablauf gestartet hat. Sie können bei der Konfiguration einer Filterbedingung die gewünschte Eigenschaft wählen. Normalerweise sollte es sich hierbei um eine Eigenschaft in Form eines Zeichenfolgewerts handeln.

VERGLEICHSWERT	BESCHREIBUNG
Geänderter Wert der Eigenschaft des Arbeitsablaufzielobjekts	Der Wert, für die Zuweisung zu einer bestimmten Eigenschaft des Zielobjekts der Anforderung, welche den Arbeitsablauf gestartet hat, angefordert wird, welcher die angeforderte Änderung an der Eigenschaft des Zielobjekts darstellt. Sie können bei der Konfiguration einer Filterbedingung die gewünschte Eigenschaft wählen. Normalerweise sollte es sich hierbei um eine Eigenschaft in Form eines Zeichenfolgewerts handeln.
Eigenschaft des Objekts aus dem Arbeitsablaufdatenkontext	Der Wert einer bestimmten Eigenschaft des Objekts, welches durch die Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt wird. Bei der Konfiguration einer Filterbedingung in einer Suchaktivität können Sie die gewünschte Eigenschaft wählen und angeben, welches Objekt von der Aktivität nach Auswertung der Bedingung zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll.
Durch Regel-Ausdruck generierter Wert	Der Zeichenfolgewert eines bestimmten Regel-Ausdrucks. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden.
Festes Objekt im Verzeichnis	Ein bestimmtes Objekt, wie etwa ein Benutzer, eine Gruppe oder ein Computer. Sie können das gewünschte Objekt in Active Directory bei der Konfiguration einer Filterbedingung wählen. Dieser Vergleichswert ist anwendbar auf Filterbedingungen für DN-Wert-Eigenschaften.
Objekt aus dem Arbeitsablaufdatenkontext	Das Objekt, welches durch die Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt wird. Bei der Konfiguration einer Filterbedingung in einer Suchaktivität können Sie angeben, welches Objekt von der Aktivität nach Auswertung der Bedingung zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll. Dieser Vergleichswert ist anwendbar auf Filterbedingungen für DN-Wert-Eigenschaften.
Durch Regel-Ausdruck des DN-Wertes identifiziertes Objekt	Das Objekt, dessen eindeutiger Name (Distinguished Name, DN) vom Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben wird. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration einer Filterbedingung erstellen. Dieser Vergleichswert ist anwendbar auf Filterbedingungen für DN-Wert-Eigenschaften.
Vom Arbeitsablaufparameter erkanntes Objekt	Das Objekt, das durch einen bestimmten Parameterwert angegeben wird. Sie können bei der Konfiguration einer Filterbedingung den gewünschten Parameter wählen. Dieser Vergleichswert ist anwendbar auf Filterbedingungen für DN-Wert-Eigenschaften.
Objekt des Arbeitsablaufinitiators	Das Benutzerkonto des Benutzers, dessen Anforderung den Arbeitsablauf gestartet hat. Dieser Vergleichswert ist anwendbar auf Filterbedingungen für DN-Wert-Eigenschaften.
Arbeitsablaufzielobjekt	Das Zielobjekt der Anforderung, die den Arbeitsablauf gestartet hat. Dieser Vergleichswert ist anwendbar auf Filterbedingungen für DN-Wert-Eigenschaften.
Festes Datum und feste Uhrzeit	Datum und Uhrzeit als Literalwerte. Sie können bei der Konfiguration einer Filterbedingung das gewünschte Datum und die gewünschte Uhrzeit wählen. Dieser Vergleichswert ist anwendbar auf Filterbedingungen für Eigenschaften mit einem Datum/Uhrzeit-Wert.

VERGLEICHSWERT	BESCHREIBUNG
Datum und Uhrzeit des Arbeitsablaufs	Ein bestimmter Zeitpunkt relativ zum Datum und zur Uhrzeit der Ausführung der Suchaktivität. Sie haben die Option, ein Datum anzugeben, das eine bestimmte Anzahl von Daten vor oder nach Ausführung der Suchaktivität liegt. Dieser Vergleichswert ist anwendbar auf Filterbedingungen für Eigenschaften mit einem Datum/Uhrzeit-Wert.
Richtig	Der boolesche Literalwert von Wahr.
Falsch	Der boolesche Literalwert von Falsch.
Vom Skript generierter Wert	Der Wert, der von einer bestimmten Skriptfunktion zurückgegeben wird. Sie können bei der Konfiguration einer Filterbedingung die gewünschte Skriptfunktion wählen. Die Suchaktivität wird diese Skriptfunktion nach Auswertung der Bedingung zum Ausführungszeitpunkt des Arbeitsablaufs ausführen.
Arbeitsablaufparameterwert	Der Wert eines bestimmten Arbeitsablaufsparameters. Sie können bei der Konfiguration einer Filterbedingung den gewünschten Parameter wählen.

Benachrichtigung

Sie können eine Suchaktivität darauf konfigurieren, Empfänger als Abonnenten der Benachrichtigungen folgender Ereignisse festzulegen:

- **Aktivität erfolgreich abgeschlossen.** Wenn diese Aktivität so konfiguriert wurde, dass Benachrichtigungen über dieses Ereignis erfolgen, versendet ActiveRoles eine Benachrichtigungs-E-Mail, wenn während der Ausführung dieser Aktivität keine erheblichen Fehler festgestellt wurden.
- **Aktivität hat einen Fehler festgestellt.** Wenn diese Aktivität so konfiguriert wurde, dass Benachrichtigungen über dieses Ereignis erfolgen, versendet ActiveRoles eine Benachrichtigungs-E-Mail, wenn während der Ausführung dieser Aktivität erhebliche Fehler festgestellt wurden.

Die Benachrichtigungseinstellungen geben das Ereignis an, über das eine Benachrichtigung versendet werden soll, sowie die Empfänger der Benachrichtigung. Wenn sie vom Arbeitsablauf ausgeführt wird, verfasst diese Aktivität eine dem angegebenen Ereignis entsprechende Benachrichtigung. ActiveRoles hält die von der Aktivität vorbereitete Meldung zurück und sendet die Meldung bei Eintritt des Ereignisses an die angegebenen Empfänger. Die Benachrichtigungseinstellungen sind vergleichbar mit den Benachrichtigungseinstellungen einer Benachrichtigungsaktivität (siehe Abschnitt Benachrichtigungsaktivität weiter oben in diesem Dokument).

Fehlerbehebung

Bei der Konfiguration einer Suchaktivität können Sie wählen, ob von dieser Aktivität festgestellte Fehler unterdrückt werden sollen. Die folgende Option ist verfügbar: **Arbeitsablauf fortsetzen, auch wenn bei dieser Aktivität ein Fehler festgestellt wird** Wenn diese Option nicht ausgewählt ist (Standardeinstellung), führt eine von der Aktivität festgestellte Fehlerbedingung dazu, dass ActiveRoles den Arbeitsablauf beendet. Wenn Sie diese Option auswählen, wird der Arbeitsablauf unabhängig davon fortgesetzt, ob die Suchaktivität oder eine in der Suchaktivität enthaltene Aktivität eine Fehlerbedingung feststellt oder nicht.

„Ausführen als"-Optionen

Standardmäßig wird die Suchaktivität unter dem Benutzerkonto ausgeführt, das in der Einstellung „Ausführen als" in den Optionen und Startbedingungen des Arbeitsablaufs festgelegt wurde. Dabei kann es sich um das Dienstkonto des ActiveRoles-Verwaltungsdienstes oder um das Konto des Benutzers handeln, der den Start des Arbeitsablaufs ausgelöst hat. Sie können die Aktivität darauf konfigurieren, die standardmäßige Einstellung „Ausführen als" zu überschreiben, indem Sie wählen, dass die Aktivität unter dem Dienstkonto oder dem Konto des Benutzers ausgeführt werden soll, der den Start des Arbeitsablaufs ausgelöst hat. Das Konto, unter dem die Aktivität ausgeführt wird, bestimmt die Zugriffsrechte der Aktivität im Verzeichnis.

Zusätzliche Einstellungen

Eine Suchaktivität verfügt über folgende zusätzliche Konfigurationsoptionen:

- **Suchaktivität beenden, wenn die Suche mehr als <Anzahl> Objekte zurückgibt.** Verwenden Sie diese Option, um die maximale Anzahl an Objekten anzugeben, die die Aktivität bei der Suche zurückgeben darf. Wenn Sie alle Objekte abrufen möchten, welche die Suchbedingungen erfüllen, können Sie diese Option deaktivieren.
- **Anforderungskontrollen in die Aktivitäts-Vorgangsanforderung aufnehmen oder ausschließen.** Anforderungskontrollen sind bestimmte Datenelemente in einer Vorgangsanforderungen, die verwendet werden können, um ActiveRoles zusätzliche Informationen darüber zur Verfügung zu stellen, wie die Anforderung verarbeitet werden soll. Anforderungskontrollen sind optional. Wenn keine Anforderungskontrollen zu einer Anforderung hinzugefügt werden, bestimmt ActiveRoles allein auf Basis des Anforderungstyps, wie die Anforderung verarbeitet werden soll. Sie können die Aktivität darauf konfigurieren, bestimmte Kontrollen zu den jeweiligen Vorgangsanforderungen hinzuzufügen (Anforderungskontrollen aufnehmen) oder sicherstellen, dass bestimmte Kontrollen niemals in Aktivitätsvorgangsanforderungen auftreten (Anforderungskontrollen ausschließen). Weitere Informationen zu Anforderungskontrollen in ActiveRoles finden Sie im ActiveRoles SDK.

Suchaktivität beenden

Sie können die Aktivität „Suche stoppen" in einer Suchaktivität verwenden, um die von der Suchaktivität durchgeführte Suche zu stoppen. Eine Aktivität „Suche stoppen" ist im Grunde zur Verwendung in einer Wenn-Dann-Aktivität ausgelegt, die in einer Suchaktivität verschachtelt wurde, damit die Suche gestoppt wird, wenn bestimmte Bedingungen erfüllt sind. In diesem Szenario analysiert die Wenn-Dann-Aktivität die von der Suche zurückgegebenen Daten und führt den Wenn-Dann-Zweig aus, der die Aktivität „Suche stoppen" enthält, wenn die von der Suche zurückgegebenen Daten die Bedingungen des Wenn-Dann-Zweigs erfüllen.

CRUD-Aktivitäten

ActiveRoles bietet eine Reihe an Arbeitsablauf-Aktivitäten, die gemeinhin als CRUD-Aktivitäten bezeichnet werden und darauf ausgelegt sind, neue Objekte zu erstellen und bestehende Objekte in Active Directory zu modifizieren oder zu löschen. Die CRUD-Abkürzung bezieht sich auf die Hauptvorgänge (in englischer Sprache), die mit diesen Aktivitäten durchgeführt werden können: Erstellen (Create), Lesen (Read), Aktualisieren (Update), Löschen (Delete). Die folgenden CRUD-Aktivitäten sind in ActiveRoles Workflow Designer verfügbar:

- Aktivität „Erstellen" Erstellt ein Objekt, z.B. einen Benutzer, eine Gruppe oder einen Computer, in Active Directory.
- Aktivität „Aktualisieren" Ändert die Eigenschaften eines Objekts, z.B. eines Benutzers, eines Computers oder einer Gruppe, in Active Directory.
- Aktivität „Zu einer Gruppe hinzufügen" Fügt ein Objekt, z.B. einen Benutzer, eine Gruppe oder einen Computer, in Active Directory hinzu.
- Aktivität „Aus einer Gruppe entfernen" Entfernt ein Objekt, z.B. einen Benutzer, eine Gruppe oder einen Computer, aus bestimmten Gruppen in Active Directory.
- Aktivität „Verschieben" Verschiebt ein Objekt, z.B. einen Benutzer, eine Gruppe oder einen Computer, in einen bestimmten Container in Active Directory.
- Aktivität „Deprovisionieren" Deprovisioniert einen Benutzer oder eine Gruppe durch Anwendung der Deprovisionsrichtlinie von ActiveRoles.
- Aktivität „Deprovisionierung aufheben" Stellt einen Benutzer oder eine Gruppe wieder her, der bzw. die mit Hilfe von ActiveRoles deprovisioniert wurde.
- Aktivität „Löschen" Löscht ein Objekt, z.B. einen Benutzer, einen Computer oder eine Gruppe, in Active Directory.

Die folgenden Themen in diesem Abschnitt bieten einen Überblick zu den Konfigurationseinstellungen, die gemeinhin für CRUD-Aktivitäten vorgenommen werden können:

- Benachrichtigung ActiveRoles kann eine E-Mail-Benachrichtigung dazu aussenden, ob die Aktivität zum Ausführungszeitpunkt eine Fehlerbedingung festgestellt hat oder nicht.
- Fehlerbehebung Legt fest, ob der Arbeitsablauf auch dann fortgesetzt werden darf, wenn die Aktivität zum Ausführungszeitpunkt eine Fehlerbedingung festgestellt hat.
- „Ausführen als"-Optionen Legt das Konto fest, unter dem die Aktivität ausgeführt werden soll.
- Zusätzliche Einstellungen Diverse erweiterte Konfigurationsoptionen, mit denen Sie die Verarbeitung des von der Aktivität angeforderten Vorgangs anpassen können.

Aktivität „Erstellen"

Die Aktivität „Erstellen" ist darauf ausgelegt, ein Objekt, z.B. einen Benutzer, einen Computer oder eine Gruppe, in Active Directory zu erstellen. Mit diese Aktivität können Sie die folgenden Merkmale des zu erstellenden Objekts konfigurieren:

- **Container.** Sie können die Organisationseinheit (OU) oder den Container angeben, in der bzw. dem die Aktivität ein Objekt erstellen soll. Die folgenden Optionen sind verfügbar:
  - **Fester Container in Verzeichnis.** Erstellt ein Objekt in der jeweiligen Organisationseinheit bzw. im jeweiligen Container. Sie können die gewünschte Organisationseinheit bzw. den Container in Active Directory bei der Konfiguration einer Erstellungsaktivität wählen.
  - **Aktivitätszielobjekt.** Erstellt ein Objekt in der Organisationseinheit oder im Container, die bzw. der von einer anderen CRUD-Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs erstellt oder anderweitig verarbeitet wurde. Sie können die gewünschte CRUD-Aktivität bei der Konfiguration einer Erstellungsaktivität aus der Arbeitsablaufdefinition wählen.
  - **Vom Arbeitsablaufparameter erkanntes Objekt.** Erstellt ein Objekt in der Organisationseinheit oder im Container, die bzw. der durch den Wert eines bestimmten Arbeitsablaufparameters angegeben wurde. Sie können den gewünschten Parameter bei der Konfiguration einer Erstellungsaktivität aus der Arbeitsablaufdefinition wählen.
  - **Objektes aus Arbeitsablauf-Datenkontext.** Erstellt ein Objekt in der Organisationseinheit oder im Container, die bzw. der von der Suchaktivität auf Basis der zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefundenen Daten ausgewählt wird. Bei der Konfiguration einer Erstellungsaktivität können Sie angeben, welche Organisationseinheit bzw. welcher Container von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll.
  - **Durch Regel-Ausdruck des DN-Werts identifiziertes Objekt.** Erstellt ein Objekt in der Organisationseinheit oder im Container, deren bzw. dessen eindeutiger Name (Distinguished Name, DN) vom Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben wird. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration einer Erstellungsaktivität erstellen.
- **Objekttyp und -name.** Sie können den Typ und den Namen des Objekts angeben, das von der Aktivität erstellt wird. Bei der Konfiguration einer Erstellungsaktivität können Sie den geeigneten Objekttyp wählen und definieren, wie die Aktivität bei der Objekterstellung den Namen des Objekts erzeugen soll. Die folgenden Optionen sind verfügbar:
  - **Textzeichenfolge.** Verwendet die angegebene Zeichenfolge als Objektname. Sie können die gewünschte Zeichenfolge bei der Konfiguration einer Erstellungsaktivität angeben.
  - **Arbeitsablaufparameterwert.** Der Name des Objekts wird von der Zeichenfolge eines bestimmen Arbeitsablaufsparameters angegeben. Sie können den gewünschten Parameter bei der Konfiguration einer Erstellungsaktivität aus der Arbeitsablaufdefinition wählen.
  - **Eigenschaft des Objektes aus dem Arbeitsablauf-Datenkontext.** Der Name des Objekts wird durch den Wert einer bestimmten Eigenschaft jenes Objekts identifiziert, das von der Wenn-Dann-Aktivität auf Basis der zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefundenen Daten ausgewählt wird. Bei der Konfiguration einer Erstellungsaktivität können Sie die gewünschte Eigenschaft wählen und angeben, welches Objekt von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll.

    - **Durch Regel-Ausdruck generierter Wert.** Der Name des Objekts wird durch den Zeichenfolgewert eines bestimmten Regel-Ausdrucks identifiziert. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration einer Erstellungsaktivität erstellen.
- **Objekteigenschaften.** Sie können definieren, wie die Aktivität die Eigenschaften des neuen Objekts auffüllen soll. Bei der Konfiguration einer Erstellungsaktivität können Sie die Eigenschaften wählen, die von der Aktivität aufgefüllt werden sollen, und für jede Eigenschaft den Wert angeben, der dieser Eigenschaft zugewiesen werden soll. Die folgenden Optionen sind verfügbar:
    - **Textzeichenfolge.** Verwendet die angegebene Zeichenfolge als Wert der Eigenschaft. Sie können die gewünschte Zeichenfolge bei der Konfiguration einer Erstellungsaktivität angeben.
    - **Eigenschaft des Arbeitsablaufsinitiators.** Verwendet den Wert einer bestimmten Eigenschaft des Benutzers, dessen Anforderung den Arbeitsablauf gestartet hat. Sie können die gewünschte Eigenschaft bei der Konfiguration einer Erstellungsaktivität angeben.
    - **Arbeitsablaufparameterwert.** Verwendet den Wert eines bestimmten Arbeitsablaufsparameters. Sie können den gewünschten Parameter bei der Konfiguration einer Erstellungsaktivität aus der Arbeitsablaufdefinition wählen.
    - **Eigenschaft des Objektes aus dem Arbeitsablauf-Datenkontext.** Verwendet den Wert einer bestimmten Eigenschaft jenes Objekts, das von der Erstellungsaktivität auf Basis der zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefundenen Daten ausgewählt wird. Bei der Konfiguration einer Erstellungsaktivität können Sie die gewünschte Eigenschaft wählen und angeben, welches Objekt von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll.
    - **Durch Regel-Ausdruck generierter Wert.** Verwendet den Zeichenfolgewert eines bestimmten Regel-Ausdrucks. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration einer Erstellungsaktivität erstellen.

Die Aktivität „Erstellen" verfügt ebenfalls über eine Reihe von Konfigurationseinstellungen, die gemeinhin bei CRUD-Aktivitäten verwendet werden:

- Benachrichtigung ActiveRoles kann eine E-Mail-Benachrichtigung dazu aussenden, ob die Aktivität zum Ausführungszeitpunkt eine Fehlerbedingung festgestellt hat oder nicht.
- Fehlerbehebung Legt fest, ob der Arbeitsablauf auch dann fortgesetzt werden darf, wenn die Aktivität zum Ausführungszeitpunkt eine Fehlerbedingung festgestellt hat.
- „Ausführen als"-Optionen Legt das Konto fest, unter dem die Aktivität ausgeführt werden soll.
- Zusätzliche Einstellungen Diverse erweiterte Konfigurationsoptionen, mit denen Sie die Verarbeitung des von der Aktivität angeforderten Vorgangs anpassen können.

Aktivität „Aktualisieren“

Die Aktivität „Aktualisieren“ ist darauf ausgelegt, Änderungen an bestimmten Eigenschaften eines Objekts vorzunehmen. Diese Aktivität hat die folgenden Konfigurationseinstellungen:

- **Aktivitätsziel.** Mit dieser Option können Sie das Objekt angeben, dessen Eigenschaften von der Aktivität geändert werden sollen. Sie können das Objekt bei der Konfiguration der Aktivität angeben oder aber die Aktivität darauf konfigurieren, das geeignete Objekt zum Ausführungszeitpunkt des Arbeitsablaufs auszuwählen. Siehe Aktivitätsziel für weitere Details.
- **Zieleigenschaften.** Sie können definieren, wie die Aktivität die Eigenschaften des Objekts ändern soll. Bei der Konfiguration einer Aktualisierungsaktivität können Sie die Eigenschaften wählen, die von der Aktivität geändert werden sollen, und für jede Eigenschaft den neuen Wert angeben, der dieser Eigenschaft zugewiesen werden soll. Bei Eigenschaften mit mehreren Werten können Sie sich dazu entscheiden, den Wert dieser Eigenschaft hinzuzufügen oder zu entfernen. Die folgenden Optionen sind verfügbar:
  - **Textzeichenfolge.** Verwendet die angegebene Zeichenfolge als Wert der Eigenschaft. Sie können die gewünschte Zeichenfolge bei der Konfiguration einer Aktualisierungsaktivität angeben.
  - **Eigenschaft des Arbeitsablaufsinitiators.** Verwendet den Wert einer bestimmten Eigenschaft des Benutzers, dessen Anforderung den Arbeitsablauf gestartet hat. Sie können die gewünschte Eigenschaft bei der Konfiguration einer Aktualisierungsaktivität angeben.
  - **Arbeitsablaufparameterwert.** Verwendet den Wert eines bestimmten Arbeitsablaufsparameters. Sie können den gewünschten Parameter bei der Konfiguration einer Aktualisierungsaktivität aus der Arbeitsablaufdefinition wählen.
  - **Eigenschaft des Objektes aus dem Arbeitsablauf-Datenkontext.** Verwendet den Wert einer bestimmten Eigenschaft jenes Objekts, das von der Aktualisierungsaktivität auf Basis der zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefundenen Daten ausgewählt wird. Bei der Konfiguration einer Aktualisierungsaktivität können Sie die gewünschte Eigenschaft wählen und angeben, welches Objekt von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll.
  - **Durch Regel-Ausdruck generierter Wert.** Verwendet den Zeichenfolgewert eines bestimmten Regel-Ausdrucks. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration einer Aktualisierungsaktivität erstellen.

Die Aktivität „Aktualisieren“ verfügt ebenfalls über eine Reihe von Konfigurationseinstellungen, die gemeinhin bei CRUD-Aktivitäten verwendet werden:

- Benachrichtigung ActiveRoles kann eine E-Mail-Benachrichtigung dazu aussenden, ob die Aktivität zum Ausführungszeitpunkt eine Fehlerbedingung festgestellt hat oder nicht.
- Fehlerbehebung Legt fest, ob der Arbeitsablauf auch dann fortgesetzt werden darf, wenn die Aktivität zum Ausführungszeitpunkt eine Fehlerbedingung festgestellt hat.
- „Ausführen als“-Optionen Legt das Konto fest, unter dem die Aktivität ausgeführt werden soll.
- Zusätzliche Einstellungen Diverse erweiterte Konfigurationsoptionen, mit denen Sie die Verarbeitung des von der Aktivität angeforderten Vorgangs anpassen können.

Aktivität „Zu einer Gruppe hinzufügen"

Die Aktivität „Zu einer Gruppe hinzufügen" ist darauf ausgelegt, ein Objekt, z.B. einen Benutzer, einen Computer oder eine Gruppe, zu bestimmten Gruppen in Active Directory hinzuzufügen. Diese Aktivität hat die folgenden Konfigurationseinstellungen:

- **Aktivitätsziel.** Mit dieser Option können Sie das Objekt angeben, das von der Aktivität zu Gruppen hinzugefügt werden soll. Sie können das Objekt bei der Konfiguration der Aktivität angeben oder aber die Aktivität darauf konfigurieren, das geeignete Objekt zum Ausführungszeitpunkt des Arbeitsablaufs auszuwählen. Siehe Aktivitätsziel für weitere Details.
- **Gruppen.** Mit dieser Option können Sie die Gruppen definieren, zu denen die Aktivität das Objekt hinzufügen soll. Bei der Konfiguration einer Aktivität „Zur Gruppe hinzufügen" können Sie eine Liste von Gruppen angeben. Die Aktivität wird das Objekt zu jeder Gruppe hinzufügen, die in dieser Liste aufgeführt ist. Um eine Gruppe zur Liste hinzuzufügen, können Sie aus den folgenden Optionen wählen:
  - **Feste Gruppe im Verzeichnis.** Sie können die gewünschte Gruppe bei der Konfiguration einer Aktivität „Zu Gruppe hinzufügen" in Active Directory wählen. Ein eindeutiger Kennzeichner der Gruppe wird in der Konfiguration der Aktivität gespeichert. Die Aktivität verwendet diesen Kennzeichner, um die Gruppe bei der Berechnung der Gruppenliste zum Ausführungszeitpunkt des Arbeitsablaufs auszuwählen.
  - **Objekt aus Arbeitsablauf-Datenkontext.** Die Gruppe wird von der Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt. Bei der Konfiguration einer Aktivität „Zu Gruppe hinzufügen" können Sie angeben, welche Gruppe von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll.
  - **Durch Regel-Ausdruck des DN-Wertes identifiziertes Objekt.** Der eindeutige Name (Distinguished Name, DN) der Gruppe wird durch den Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration einer Aktivität „Zu Gruppe hinzufügen" erstellen.

Die Aktivität „Zu Gruppe hinzufügen" verfügt ebenfalls über eine Reihe von Konfigurationseinstellungen, die gemeinhin bei CRUD-Aktivitäten verwendet werden:

- Benachrichtigung ActiveRoles kann eine E-Mail-Benachrichtigung dazu aussenden, ob die Aktivität zum Ausführungszeitpunkt eine Fehlerbedingung festgestellt hat oder nicht.
- Fehlerbehebung Legt fest, ob der Arbeitsablauf auch dann fortgesetzt werden darf, wenn die Aktivität zum Ausführungszeitpunkt eine Fehlerbedingung festgestellt hat.
- „Ausführen als"-Optionen Legt das Konto fest, unter dem die Aktivität ausgeführt werden soll.
- Zusätzliche Einstellungen Diverse erweiterte Konfigurationsoptionen, mit denen Sie die Verarbeitung des von der Aktivität angeforderten Vorgangs anpassen können.

Aktivität „Aus einer Gruppe entfernen"

Die Aktivität „Aus einer Gruppe entfernen" ist darauf ausgelegt, ein Objekt, z.B. einen Benutzer, einen Computer oder eine Gruppe, aus bestimmten Gruppen in Active Directory zu entfernen. Diese Aktivität hat die folgenden Konfigurationseinstellungen:

- **Aktivitätsziel.** Mit dieser Option können Sie das Objekt angeben, das von der Aktivität aus Gruppen entfernt werden soll. Sie können das Objekt bei der Konfiguration der Aktivität angeben oder aber die Aktivität darauf konfigurieren, das geeignete Objekt zum Ausführungszeitpunkt des Arbeitsablaufs auszuwählen. Siehe Aktivitätsziel für weitere Details.
- **Gruppen - Objekt aus allen Gruppen entfernen.** Diese Option konfiguriert die Aktivität darauf, das Objekt aus allen Gruppen in Active Directory zu entfernen. Beachten Sie, dass ein Objekt nicht aus der primären Gruppe des Objekts entfernt werden kann, die Aktivität entfernt das Objekt daher aus allen Gruppen außer der primären Gruppe des Objekts.
- **Gruppen - Objekt aus diesen Gruppen entfernen.** Mit dieser Option können Sie die Gruppen auflisten, aus denen die Aktivität das Objekt entfernen soll. Sie können bei der Konfiguration einer Aktivität „Aus Gruppe entfernen" eine Liste von Gruppen angeben. Die Aktivität wird das Objekt aus jeder in der Liste aufgeführten Gruppe (außer aus der primären Gruppe des Objekts) entfernen. Um eine Gruppe zur Liste hinzuzufügen, können Sie aus den folgenden Optionen wählen:
  - **Feste Gruppe im Verzeichnis.** Sie können die gewünschte Gruppe bei der Konfiguration einer Aktivität „Aus Gruppe entfernen" in Active Directory wählen. Ein eindeutiger Kennzeichner der Gruppe wird in der Konfiguration der Aktivität gespeichert. Die Aktivität verwendet diesen Kennzeichner, um die Gruppe bei der Berechnung der Gruppenliste zum Ausführungszeitpunkt des Arbeitsablaufs auszuwählen.
  - **Objekt aus Arbeitsablauf-Datenkontext.** Die Gruppe wird von der Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt. Bei der Konfiguration einer Aktivität „Aus Gruppe entfernen" können Sie angeben, welche Gruppe von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll.
  - **Durch Regel-Ausdruck des DN-Wertes identifiziertes Objekt.** Der eindeutige Name (Distinguished Name, DN) der Gruppe wird durch den Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration einer Aktivität „Aus Gruppe entfernen" erstellen.

Die Aktivität „Aus Gruppe entfernen" verfügt ebenfalls über eine Reihe von Konfigurationseinstellungen, die gemeinhin bei CRUD-Aktivitäten verwendet werden:

- Benachrichtigung ActiveRoles kann eine E-Mail-Benachrichtigung dazu aussenden, ob die Aktivität zum Ausführungszeitpunkt eine Fehlerbedingung festgestellt hat oder nicht.
- Fehlerbehebung Legt fest, ob der Arbeitsablauf auch dann fortgesetzt werden darf, wenn die Aktivität zum Ausführungszeitpunkt eine Fehlerbedingung festgestellt hat.
- „Ausführen als"-Optionen Legt das Konto fest, unter dem die Aktivität ausgeführt werden soll.
- Zusätzliche Einstellungen Diverse erweiterte Konfigurationsoptionen, mit denen Sie die Verarbeitung des von der Aktivität angeforderten Vorgangs anpassen können.

Aktivität „Verschieben"

Die Aktivität „Verschieben" ist darauf ausgelegt, ein bestimmtes Objekt in einen Container in Active Directory zu verschieben. Die Aktivität hat die folgenden Konfigurationseinstellungen:

- **Aktivitätsziel.** Mit dieser Option können Sie das Objekt angeben, das von der Aktivität verschoben werden soll. Sie können das Objekt bei der Konfiguration der Aktivität angeben oder aber die Aktivität darauf konfigurieren, das geeignete Objekt zum Ausführungszeitpunkt des Arbeitsablaufs auszuwählen. Siehe Aktivitätsziel für weitere Details.
- **Zielcontainer.** Sie können die Organisationseinheit (OU) oder den Container angeben, in die bzw. den die Aktivität ein Objekt verschieben soll. Die folgenden Optionen sind verfügbar:
  - **Fester Container in Verzeichnis.** Verschiebt ein Objekt in die jeweilige Organisationseinheit bzw. in den jeweiligen Container. Sie können die gewünschte Organisationseinheit bzw. den Container in Active Directory bei der Konfiguration einer Verschiebungsaktivität wählen.
  - **Aktivitätszielobjekt.** Verschiebt ein Objekt in die Organisationseinheit oder in den Container, die bzw. der von einer anderen CRUD-Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs erstellt oder anderweitig verarbeitet wurde. Sie können die gewünschte CRUD-Aktivität bei der Konfiguration einer Verschiebungsaktivität aus der Arbeitsablaufdefinition wählen.
  - **Vom Arbeitsablaufparameter erkanntes Objekt.** Verschiebt ein Objekt in die Organisationseinheit oder in den Container, die bzw. der durch den Wert eines bestimmten Arbeitsablaufparameters angegeben wurde. Sie können den gewünschten Parameter bei der Konfiguration einer Verschiebungsaktivität aus der Arbeitsablaufdefinition wählen.
  - **Objektes aus Arbeitsablauf-Datenkontext.** Verschiebt ein Objekt in die Organisationseinheit oder den Container, die bzw. der von der Suchaktivität auf Basis der zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefundenen Daten ausgewählt wird. Bei der Konfiguration einer Verschiebungsaktivität können Sie angeben, welche Organisationseinheit bzw. welcher Container von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll.
  - **Durch Regel-Ausdruck des DN-Werts identifiziertes Objekt.** Verschiebt ein Objekt in die Organisationseinheit oder in den Container, deren bzw. dessen eindeutiger Name (Distinguished Name, DN) vom Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben wird. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration einer Verschiebungsaktivität erstellen.

Die Aktivität „Verschieben" verfügt ebenfalls über eine Reihe von Konfigurationseinstellungen, die gemeinhin bei CRUD-Aktivitäten verwendet werden:

- Benachrichtigung ActiveRoles kann eine E-Mail-Benachrichtigung dazu aussenden, ob die Aktivität zum Ausführungszeitpunkt eine Fehlerbedingung festgestellt hat oder nicht.
- Fehlerbehebung Legt fest, ob der Arbeitsablauf auch dann fortgesetzt werden darf, wenn die Aktivität zum Ausführungszeitpunkt eine Fehlerbedingung festgestellt hat.
- „Ausführen als"-Optionen Legt das Konto fest, unter dem die Aktivität ausgeführt werden soll.
- Zusätzliche Einstellungen Diverse erweiterte Konfigurationsoptionen, mit denen Sie die Verarbeitung des von der Aktivität angeforderten Vorgangs anpassen können.

Aktivität „Deprovisionieren"

Die Aktivität „Deprovisionieren" ist darauf ausgelegt, die Deprovisionierungsrichtlinien von ActiveRoles auf einen bestimmten Benutzer oder eine bestimmte Gruppe anzuwenden. Mit dieser Aktivität führt ActiveRoles alle von den Deprovisionierungsrichtlinien vorgeschriebenen Aufgaben aus und deprovisioniert so den Benutzer oder die Gruppe.

Die Aktivität ermöglicht es Ihnen, das Benutzer- oder Gruppenobjekt anzugeben, das von der Aktivität deprovisioniert werden soll. Sie können das Objekt bei der Konfiguration der Aktivität angeben oder aber die Aktivität darauf konfigurieren, das geeignete Objekt zum Ausführungszeitpunkt des Arbeitsablaufs auszuwählen. Siehe Aktivitätsziel für weitere Details.

Die Aktivität „Deprovisionieren" verfügt ebenfalls über eine Reihe von Konfigurationseinstellungen, die gemeinhin bei CRUD-Aktivitäten verwendet werden:

- Benachrichtigung ActiveRoles kann eine E-Mail-Benachrichtigung dazu aussenden, ob die Aktivität zum Ausführungszeitpunkt eine Fehlerbedingung festgestellt hat oder nicht.
- Fehlerbehebung Legt fest, ob der Arbeitsablauf auch dann fortgesetzt werden darf, wenn die Aktivität zum Ausführungszeitpunkt eine Fehlerbedingung festgestellt hat.
- „Ausführen als"-Optionen Legt das Konto fest, unter dem die Aktivität ausgeführt werden soll.
- Zusätzliche Einstellungen Diverse erweiterte Konfigurationsoptionen, mit denen Sie die Verarbeitung des von der Aktivität angeforderten Vorgangs anpassen können.

Aktivität „Deprovisionierung aufheben"

Die Aktivität „Deprovisionierung aufheben" ist darauf ausgelegt, einen bestimmten Benutzer oder eine bestimmte Gruppe wiederherzustellen, die mit Hilfe von ActiveRoles deprovisioniert wurde. Mit dieser Aktivität macht ActiveRoles die Änderungen rückgängig, die am Benutzer- oder Gruppenobjekt durch die Anwendung der Deprovisionierungsrichtlinien von ActiveRoles vorgenommen wurden. Daher wird das Objekt in den Zustand zurückversetzt, in dem es sich befand, bevor die deprovisionierungsbezogenen Änderungen vorgenommen wurden.

Die Aktivität ermöglicht es Ihnen, das Benutzer- oder Gruppenobjekt anzugeben, das von der Aktivität wiederhergestellt werden soll. Sie können das Objekt bei der Konfiguration der Aktivität angeben oder aber die Aktivität darauf konfigurieren, das geeignete Objekt zum Ausführungszeitpunkt des Arbeitsablaufs auszuwählen. Siehe Aktivitätsziel für weitere Details.

Die Aktivität „Deprovisionierung aufheben" verfügt ebenfalls über eine Reihe von Konfigurationseinstellungen, die gemeinhin bei CRUD-Aktivitäten verwendet werden:

- Benachrichtigung ActiveRoles kann eine E-Mail-Benachrichtigung dazu aussenden, ob die Aktivität zum Ausführungszeitpunkt eine Fehlerbedingung festgestellt hat oder nicht.
- Fehlerbehebung Legt fest, ob der Arbeitsablauf auch dann fortgesetzt werden darf, wenn die Aktivität zum Ausführungszeitpunkt eine Fehlerbedingung festgestellt hat.
- „Ausführen als"-Optionen Legt das Konto fest, unter dem die Aktivität ausgeführt werden soll.
- Zusätzliche Einstellungen Diverse erweiterte Konfigurationsoptionen, mit denen Sie die Verarbeitung des von der Aktivität angeforderten Vorgangs anpassen können.

Aktivität „Löschen"

Die Aktivität „Löschen" ist darauf ausgelegt, ein bestimmtes Objekt in Active Directory zu löschen. Die Aktivität ermöglicht es Ihnen, das Objekt anzugeben, das von der Aktivität gelöscht werden soll. Sie können das Objekt bei der Konfiguration der Aktivität angeben oder aber die Aktivität darauf konfigurieren, das geeignete Objekt zum Ausführungszeitpunkt des Arbeitsablaufs auszuwählen. Siehe Aktivitätsziel für weitere Details.

Die Aktivität „Löschen" verfügt ebenfalls über eine Reihe von Konfigurationseinstellungen, die gemeinhin bei CRUD-Aktivitäten verwendet werden:

- Benachrichtigung ActiveRoles kann eine E-Mail-Benachrichtigung dazu aussenden, ob die Aktivität zum Ausführungszeitpunkt eine Fehlerbedingung festgestellt hat oder nicht.
- Fehlerbehebung Legt fest, ob der Arbeitsablauf auch dann fortgesetzt werden darf, wenn die Aktivität zum Ausführungszeitpunkt eine Fehlerbedingung festgestellt hat.
- „Ausführen als"-Optionen Legt das Konto fest, unter dem die Aktivität ausgeführt werden soll.
- Zusätzliche Einstellungen Diverse erweiterte Konfigurationsoptionen, mit denen Sie die Verarbeitung des von der Aktivität angeforderten Vorgangs anpassen können.

Aktivitätsziel

Die Ausführung einer CRUD-Aktivität führt zu einer Anforderung, einen bestimmten Vorgang auf einem bestimmten Objekt auszuführen. Zum Beispiel fordert eine Aktivität „Aktualisieren" ActiveRoles an, Änderungen an den Eigenschaften eines bestimmten Objekts vorzunehmen, eine Aktivität „Zu Gruppe hinzufügen" fordert ActiveRoles an, ein bestimmtes Objekt zu bestimmten Gruppen hinzuzufügen, und so weiter. Das Objekt, auf dem der von einer CRUD-Aktivität angeforderte Vorgang ausgeführt werden soll, wird das Zielobjekt dieser Aktivität genannt, oder einfach *Aktivitätsziel*.

Bei der Konfiguration einer CRUD-Aktivität können Sie die folgenden Optionen verwenden, um das Aktivitätsziel für diese Aktivität anzugeben:

- **Festes Objekt im Verzeichnis.** Das Aktivitätsziel ist das angegebene Objekt. Sie können das gewünschte Objekt in Active Directory bei der Konfiguration einer CRUD-Aktivität wählen.
- **Vom Arbeitsablaufparameter erkanntes Objekt.** Das Aktivitätsziel ist das Objekt, welches durch den Wert eines bestimmten Arbeitsablaufsparameters angegeben wurde. Sie können den gewünschten Parameter bei der Konfiguration einer CRUD-Aktivität aus der Arbeitsablaufdefinition wählen.
- **Objekt aus Arbeitsablauf-Datenkontext.** Das Aktivitätsziel wird von der Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt. Bei der Konfiguration einer CRUD-Aktivität können Sie angeben, welches Objekt von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll.
- **Durch Regel-Ausdruck des DN-Wertes identifiziertes Objekt.** Der eindeutige Name (Distinguished Name, DN) des Aktivitätsziels wird durch den Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration einer CRUD-Aktivität erstellen.

Die folgende Tabelle hilft Ihnen dabei, CRUD-Aktivitätsziele zu unterscheiden.

AKTIVITÄT	AKTIVITÄTSZIEL
Aktualisieren	Das Objekt, dessen Eigenschaften geändert werden sollen. Eine Aktualisierungsaktivität fordert ActiveRoles an, bestimmte Eigenschaften eines bestimmten Objekts zu ändern. Dieses Objekt wird das Aktivitätsziel der Aktualisierungsaktivität genannt.
Zur Gruppe hinzufügen	Das zu den Gruppen hinzuzufügende Objekt. Eine Aktivität „Zu Gruppe hinzufügen" fordert ActiveRoles an, ein bestimmtes Objekt zu bestimmten Gruppen hinzuzufügen. Dieses Objekt wird das Aktivitätsziel der Aktivität „Zu Gruppe hinzufügen" genannt.
Aus der Gruppe entfernen	Das aus den Gruppen zu entfernende Objekt. Eine Aktivität „Aus Gruppe entfernen" fordert ActiveRoles an, ein bestimmtes Objekt aus bestimmten Gruppen zu entfernen. Dieses Objekt wird das Aktivitätsziel der Aktivität „Aus Gruppe entfernen" genannt.
Verschieben	Das zu verschiebende Objekt. Eine Verschiebungsaktivität fordert ActiveRoles an, ein bestimmtes Objekt in einen bestimmten Container in Active Directory zu verschieben. Dieses Objekt wird das Aktivitätsziel der Verschiebungsaktivität genannt.
Deprovisionierung	Das zu deprovisionierende Objekt. Eine Deprovisionierungsaktivität fordert ActiveRoles an, ein bestimmtes Objekt zu deprovisionieren. Dieses Objekt wird das Aktivitätsziel der Deprovisonierungsaktivität genannt.
Deprovisionierung aufheben	Das wiederherzustellende Objekt. Eine Aktivität „Deprovisionierung aufheben" fordert ActiveRoles an, ein bestimmtes Objekt wiederherzustellen, das deprovisioniert wurde. Dieses Objekt wird das Aktivitätsziel der Aktivität „Deprovisionierung aufheben" genannt.
Löschen	Das zu löschende Objekt. Eine Löschaktivität fordert ActiveRoles an, ein bestimmtes Objekt zu löschen. Dieses Objekt wird das Aktivitätsziel der Löschaktivität genannt.

Benachrichtigung

Sie können eine CRUD-Aktivität darauf konfigurieren, Empfänger als Abonnenten der Benachrichtigungen folgender Ereignisse festzulegen:

- **Aktivität erfolgreich abgeschlossen.** Wenn diese Aktivität so konfiguriert wurde, dass Benachrichtigungen über dieses Ereignis erfolgen, versendet ActiveRoles eine Benachrichtigungs-E-Mail, wenn während der Ausführung dieser Aktivität keine erheblichen Fehler festgestellt wurden.
- **Aktivität hat einen Fehler festgestellt.** Wenn diese Aktivität so konfiguriert wurde, dass Benachrichtigungen über dieses Ereignis erfolgen, versendet ActiveRoles eine Benachrichtigungs-E-Mail, wenn während der Ausführung dieser Aktivität erhebliche Fehler festgestellt wurden.

Die Benachrichtigungseinstellungen geben das Ereignis an, über das eine Benachrichtigung versendet werden soll, sowie die Empfänger der Benachrichtigung. Wenn sie vom Arbeitsablauf ausgeführt wird, verfasst diese Aktivität eine dem angegebenen Ereignis entsprechende Benachrichtigung. ActiveRoles hält die von der Aktivität vorbereitete Meldung zurück und sendet die Meldung bei Eintritt des Ereignisses an die angegebenen Empfänger. Die Benachrichtigungseinstellungen sind vergleichbar mit den Benachrichtigungseinstellungen einer Benachrichtigungsaktivität (siehe Abschnitt Benachrichtigungsaktivität weiter oben in diesem Dokument).

Fehlerbehebung

Bei der Konfiguration einer CRUD-Aktivität können Sie wählen, ob von dieser Aktivität festgestellte Fehler unterdrückt werden sollen. Die folgende Option ist verfügbar: **Arbeitsablauf fortsetzen, auch wenn bei dieser Aktivität ein Fehler festgestellt wird** Wenn diese Option nicht ausgewählt ist (Standardeinstellung), führt eine von der Aktivität festgestellte Fehlerbedingung dazu, dass ActiveRoles den Arbeitsablauf beendet.

Wenn Sie eine CRUD-Aktivität so konfigurieren, dass der Arbeitsablauf auch dann fortgesetzt werden darf, wenn die Aktivität eine Fehlerbedingung feststellt, kann der Arbeitsablauf eine geeignete Kompensierungsaktion vornehmen. Dies kann durch die Verwendung einer Wenn-Dann-Aktivität mit einer Zweigbedingung bewerkstelligt werden, welche den Ausführungsstatus „Fehler festgestellt" der CRUD-Aktivität auswertet. Fügen Sie nach der CRUD-Aktivität eine Wenn-Dann-Aktivität hinzu und konfigurieren Sie eine Bedingung auf einem Wenn-Dann-Zweig darauf, den Ausführungsstatus „Fehler festgestellt" dieser CRUD-Aktivität zu erkennen. Konfigurieren Sie denn Wenn-Dann-Zweig dann so, dass er die Aktivitäten enthält, die von der Kompensierungsaktion durchgeführt werden sollen. Wenn so die CRUD-Aktivität einen Fehler feststellt, wird die Zweigbedingung „Fehler festgestellt" auf WAHR ausgewertet, wodurch der Arbeitsablauf den Aktivitätszweig ausführt, der die Kompensierungsaktion durchführen soll.

„Ausführen als"-Optionen

Standardmäßig wird jede CRUD-Aktivität unter dem Benutzerkonto ausgeführt, das in der Einstellung „Ausführen als" in den Optionen und Startbedingungen des Arbeitsablaufs festgelegt wurde. Dabei kann es sich um das Dienstkonto des ActiveRoles-Verwaltungsdienstes oder um das Konto des Benutzers handeln, der den Start des Arbeitsablaufs ausgelöst hat. Sie können die Aktivität darauf konfigurieren, die standardmäßige Einstellung „Ausführen als" zu überschreiben, indem Sie wählen, dass die Aktivität unter dem Dienstkonto oder dem Konto des Benutzers ausgeführt werden soll, der den Start des Arbeitsablaufs ausgelöst hat. Das Konto, unter dem die Aktivität ausgeführt wird, bestimmt die Zugriffsrechte der Aktivität im Verzeichnis.

Eine weitere Option legt fest, ob auf den von der Aktivität angeforderten Vorgang Genehmigungsregeln anzuwenden sind, wenn die Aktivität unter einem berechtigten Konto ausgeführt wird, wie etwa einem ActiveRoles-Dienstkonto, einem ActiveRoles-Administratorkonto oder dem Konto des Benutzers, der als Genehmiger bestimmt wurde. Standardmäßig verwendet die Aktivität die Einstellung, die in den Arbeitsablaufoptionen und Startbedingungen festgelegt wurde. Die Einstellung für alle Arbeitsabläufe kann jedoch für individuelle Aktivitäten überschrieben werden.

Bei der Konfiguration einer CRUD-Aktivität können Sie die Option **Genehmigung erzwingen** für diese Aktivität aktivieren oder deaktivieren. Wird sie aktiviert, führt diese Option zur Anwendung der Genehmigungsregeln und reicht den Vorgang zur Genehmigung ein, unabhängig vom Konto, unter dem die Aktivität ausgeführt wird. Ansonsten umgeht der von der Aktivität angeforderte Vorgang die Genehmigungsregeln, wenn die Aktivität unter dem ActiveRoles-Dienstkonto, einem ActiveRoles-Administratorkonto oder unter dem Konto des Benutzers ausgeführt wird, der als Genehmiger bestimmt wurde. Somit wird der Vorgang nicht zur Genehmigung eingereicht.

Zusätzliche Einstellungen

Eine CRUD-Aktivität verfügt über folgende zusätzliche Konfigurationsoptionen:

- **Diesen Text anstelle des ursprünglichen Texts für die Vorgangsbegründung verwenden.** Wenn der von der CRUD-Aktivität angeforderte Vorgang zur Genehmigung eingereicht werden muss, können Sie den Begründungstext für den Vorgang angeben, der dem Genehmiger anstatt jenes Begründungstextes angezeigt wird, welcher in der Vorgangsanforderung angegeben wurde, die den Arbeitsablauf gestartet hat. Die Unteroption **Nur dann verwenden, wenn der Grund für den Vorgang ursprünglich nicht angegeben wurde** konfiguriert die Aktivität darauf, den Begründungstext nur dann zu ersetzen, wenn für die Vorgangsanforderung, die den Arbeitsablauf gestartet hat, kein Begründungstext angegeben wurde.
- **Zulassen, dass die durch diese Aktivität erstellte Anforderung eine neue Instanz des Arbeitsablaufs, die diese Aktivität enthält, startet.** Diese Option ist normalerweise deaktiviert, um eine wiederholte Ausführung der CRUD-Aktivität in Fällen zu verhindern, bei denen der von dieser Aktivität angeforderte Vorgang in einem bestimmten Arbeitsablauf die Startbedingungen für diesen Arbeitsablauf erfüllt. Mit der Aktivierung dieser Option könnte eine Schleife von Arbeitsablaufinstanzen entstehen, welche die selbe Aktivität wieder und wieder ausführen und damit früher oder später zu einer Überlaufbedingung führen würden.
- **Anforderungskontrollen in die Aktivitäts-Vorgangsanforderung aufnehmen oder ausschließen.** Anforderungskontrollen sind bestimmte Datenelemente in einer Vorgangsanforderungen, die verwendet werden können, um ActiveRoles zusätzliche Informationen darüber zur Verfügung zu stellen, wie die Anforderung verarbeitet werden soll. Anforderungskontrollen sind optional. Wenn keine Anforderungskontrollen zu einer Anforderung hinzugefügt werden, bestimmt ActiveRoles allein auf Basis des Anforderungstyps, wie die Anforderung verarbeitet werden soll. Sie können die Aktivität darauf konfigurieren, bestimmte Kontrollen zu den jeweiligen Vorgangsanforderungen hinzuzufügen (Anforderungskontrollen aufnehmen) oder sicherstellen, dass bestimmte Kontrollen niemals in Aktivitätsvorgangsanforderungen auftreten (Anforderungskontrollen ausschließen). Weitere Informationen zu Anforderungskontrollen in ActiveRoles finden Sie im ActiveRoles SDK.

Konfigurieren eines Arbeitsablaufs

Die Workflows sind ein leistungsfähiges und praktisches Mittel, um eine neue Logik in den Directory-Datenmanagement- und -bereitstellungsprozessen in Quest One ActiveRoles hinzuzufügen. Um einen Arbeitsablauf zu konfigurieren, erstellen Sie eine Arbeitsablaufdefinition und verwenden dann den Workflow Designer, um Arbeitsablaufaktivitäten hinzuzufügen und zu konfigurieren.

Dieser Abschnitt deckt die folgenden Aufgaben ab:

- Erstellen einer Arbeitsablaufdefinition
- Konfiguration der Workflow-Start-Bedingungen
- Workflow-Parameter konfigurieren
- Hinzufügen von Aktivitäten zu einem Arbeitsablauf
- Konfigurieren einer Genehmigungsaktivität
- Konfigurieren einer Benachrichtigungsaktivität
- Konfigurieren einer Skriptaktivität
- Konfigurieren einer Wenn-Dann-Sonst-Aktivität
- Konfigurieren einer Stoppen/Unterbrechen-Aktivität
- Konfiguration einer Aktivität „Berichtsabschnitt hinzufügen"
- Konfigurieren einer Suchaktivität
- Konfiguration von CRUD-Aktivitäten
- Aktivieren oder Deaktivieren einer Aktivität
- Aktivieren oder Deaktivieren eines Arbeitsablaufs

Erstellen einer Arbeitsablaufdefinition

Die Quest One ActiveRoles-Konsole stellt den Workflow-Designer für die Erstellung und Konfiguration der Workflows bereit. Zunächst erstellen Sie eine Arbeitsablaufdefinition. Dann verwenden Sie den Workflow Designer, um einen Arbeitsablauf zu erstellen und die Arbeitsablauf-Konfigurationsdaten in der Arbeitsablaufdefinition zu speichern.

Gehen Sie folgendermaßen vor, um eine Arbeitsablaufdefinition zu erstellen:

1. Erweitern Sie in der Quest One ActiveRoles-Konsolenstruktur den Eintrag **Configuration | Policies**, klicken Sie mit der rechten Maustaste auf **Workflow** und wählen Sie **Neu | Arbeitsablaufrichtlinie**.
2. Bitte befolgen Sie die Schritte im Assistenten, um die Workflow-Definition zu erstellen.
3. Akzeptieren Sie auf der **Workflow-Typ**-Seite die Standardeinstellungen.

Standardmäßig erstellt der Assistent einen so genannten *Änderungs-Workflow*, dessen Ausführung nach einer Aufforderung, die Daten im Verzeichnis zu ändern, beginnt. Eine andere Möglichkeit besteht darin, einen *Automatisierungs-Workflow* zu erstellen, der nach einem Zeitplan synchronisiert oder nach einer Benutzeraufforderung ausgeführt werden kann. Siehe Automatisierungs-Arbeitsablauf für weitere Details.

Wenn Sie eine Workflow-Definition erstellt haben, können Sie sie im Workflow-Designer öffnen, um Workflow-Aktivitäten hinzuzufügen und die Bedingungen für den Beginn des Workflows anzugeben.

Sie können Container erstellen, um verknüpfte Workflows und andere Container zu speichern. Um einen Workflow-Container zu erstellen, klicken Sie mit der rechten Maustaste auf **Workflow** in der Konsolenstruktur und wählen Sie **Neu | Container**. Um eine Workflow-Definition in einem bestimmten Container zu erstellen, klicken Sie mit der rechten Maustaste in die Konsolenstruktur und wählen Sie **Neu | Workflow**.

Gehen Sie folgendermaßen vor, um eine Arbeitsablaufdefinition zu löschen: Klicken Sie in der Konsolenstruktur unter **Konfiguration | Richtlinien | Arbeitsablauf** mit der rechten Maustaste auf das Objekt, das die Arbeitsablaufdefinition angibt, und klicken Sie dann auf **Löschen**.

Konfiguration der Workflow-Start-Bedingungen

Die Arbeitsablauf-Startbedingungen legen fest, welche Vorgänge zum Start des Arbeitsablaufs führen. Ein Genehmigungs-Arbeitsablauf kann zum Beispiel so konfiguriert sein, dass jede Anforderung zur Erstellung eines Benutzers in einem bestimmten Container den Arbeitsablauf startet und somit die Genehmigung für die Anforderung erfordert. Sie können die Startbedingungen für einen Arbeitsablauf festlegen, indem Sie seine Definition im Workflow Designer bearbeiten.

Gehen Sie folgendermaßen vor, um die Startbedingungen für einen Arbeitsablauf anzuzeigen oder zu ändern:

1. Erweitern Sie in der Quest One ActiveRoles-Konsolenstruktur **Konfiguration | Richtlinien | Workflow** und wählen Sie den Workflow, den Sie konfigurieren möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.
2. Klicken Sie im Bereich „Details" auf die Schaltfläche **Optionen und Startbedingungen des Arbeitsablaufs**, um den Bereich über dem Prozessdiagramm zu erweitern, und klicken Sie dann auf die Schaltfläche **Konfigurieren**.
3. Klicken Sie auf den **Bedingungen**-Tab im Dialogfeld **Änderungs-Workflow-Optionen und Startbedingungen**.

Auf der erscheinenden Seite können Sie Folgendes anzeigen oder ändern:

- Vorgangsbedingungen
- Initiatorenbedingungen
- Filterbedingungen
- Optionen „Ausführen als"

Vorgangsbedingungen

Die Vorgangsbedingungen legen Folgendes fest:

- Einen Objekttyp wie etwa „Benutzer", „Gruppe" oder „Computer"; der Arbeitsablauf startet nur dann, wenn ein Vorgang Änderungen an einem Objekt dieses Typs anfordert.
- Einen Vorgangstyp wie etwa „Erstellen", „Umbenennen", „Ändern" oder „Löschen"; der Arbeitsablauf startet nur dann, wenn ein Vorgang dieses Typs angefordert wird.
- Für den Vorgangstyp „Ändern" eine Liste der Objekteigenschaften; der Arbeitsablauf startet nur dann, wenn ein Vorgang Änderungen an irgendeiner dieser Eigenschaften eines Objekts anfordert.

Gehen Sie folgendermaßen vor, um die Vorgangsbedingungen anzuzeigen oder zu ändern:

1. Gehen Sie im Dialogfeld **Änderungs-Workflow-Optionen und Startbedingungen** in den **Bedingungen**-Tab und klicken Sie auf **Vorgang wählen** im Bereich **Vorgangsbedingungen**.

   Hierdurch wird eine Seite geöffnet, auf der Sie den Objekttyp und die Vorgangstypeinstellungen anzeigen oder ändern können.

2. Um die Objekttypeinstellungen zu ändern, wählen Sie einen Objekttyp aus dem Dropdown-Listenfeld aus.

   Um einen Objekttyp auszuwählen, der nicht im Dropdown-Listenfeld enthalten ist, klicken Sie auf die Schaltfläche neben dem Dropdown-Listenfeld.

3. Um die Vorgangstypeinstellung zu ändern, klicken Sie auf die entsprechende Option.
4. Wenn der Vorgangstyp „Ändern" (die Option **Eigenschaften ändern**) ausgewählt ist, klicken Sie auf **Weiter**, um die Auswahl der Eigenschaften anzuzeigen oder zu ändern.
5. Klicken Sie auf **Fertig stellen**.

Initiatorenbedingungen

Die Initiatorbedingungen legen Folgendes fest:

- Die Identität eines Vorgangsanforderers (Initiators), z.B. Benutzer oder Gruppe; der Workflow beginnt erst, wenn ein Vorgang von dieser Identität angefordert wurde.
- Container wie etwa eine Organisationseinheit oder eine verwaltete Einheit; der Arbeitsablauf startet nur dann, wenn ein Vorgang Änderungen an bzw. die Erstellung von einem Objekt in diesem Container anfordert.

Gehen Sie folgendermaßen vor, um die Initiatorbedingungen anzuzeigen oder zu ändern:

1. Gehen Sie im Dialogfeld **Änderungs-Workflow-Optionen und Startbedingungen** in den **Bedingungen**-Tab und beobachten Sie die Liste im Bereich **Initiator-Bedingungen**.

   Jeder Eintrag in der Liste steht für eine einzelne Initiatorbedingung, wobei das erste Feld den Vorgangsanforderer und das zweite Feld den Container angibt. Wenn keine Liste vorhanden ist, sind keine Initiatorbedingungen definiert.

2. Gehen Sie folgendermaßen vor, um eine Initiatorbedingung zu definieren:
   a) Klicken Sie auf **Hinzufügen** im Bereich **Initiatorbedingungen**.
   b) Füllen Sie die Liste der Vorgangsanforderer aus.
   c) Wählen Sie den Container.
3. Um eine Initiatorbedingung zu löschen, wählen Sie den entsprechenden Eintrag aus der Liste **Initiatorbedingungen** aus und klicken Sie dann auf **Entfernen**.

Wenn mehrere Initiatorbedingungen definiert sind, startet der Arbeitsablauf, wenn eine dieser Bedingungen erfüllt ist.

Wenn mehrere Vorgangsanforderer innerhalb einer einzigen Initiatorbedingung definiert sind, wird die Bedingung als erfüllt betrachtet, wenn der Vorgang von einer dieser Identitäten angefordert wird.

Filterbedingungen

Ein Filter kann verwendet werden, um jegliche zusätzlichen Bedingungen für die an einem Vorgang beteiligten Objekte zu definieren. Der Arbeitsablauf startet nur dann, wenn der Vorgang diesen Bedingungen entspricht. Wenn kein Filter festgelegt ist, dann sind keine zusätzlichen Bedingungen gültig.

Wenn Sie einen Filter konfigurieren, müssen Sie mindestens eine Bedingung hinzufügen. Die Anzahl der Bedingungen, die Sie hinzufügen können, ist jedoch nicht beschränkt. Sie können Bedingungen mittels verschiedener Operatoren hinzufügen, löschen und gruppieren. Es ist möglich, Bedingungsgruppen in anderen Bedingungsgruppen zu verschachteln, um die gewünschten Ergebnisse zu erreichen.

Eine Bedingungsgruppe enthält eine oder mehrere Bedingungen, die durch denselben logischen Operator miteinander verbunden sind. Durch die Gruppierung von Bedingungen geben Sie an, dass diese Bedingungen als eine Einheit bewertet werden sollen. Der Effekt ist derselbe, als wenn Sie einen Ausdruck in einer mathematischen Gleichung oder in einer logischen Aussage in Klammern setzen.

Standardmäßig wird eine einzelne Bedingungsgruppe erstellt, wenn Sie eine Bedingung hinzufügen. Sie können weitere Bedingungsgruppen erstellen, um eine Reihe von Bedingungen zu gruppieren und um gruppierte Bedingungen innerhalb anderer Bedingungsgruppen zu verschachteln.

In einer Bedingungsgruppe sind die Bedingungen über die logischen Operatoren AND, OR, NOT AND oder NOT OR miteinander verknüpft:

- Die AND-Gruppe ergibt TRUE (wahr), wenn alle Bedingungen in der Gruppe TRUE (wahr) sind.
- Die ODER Gruppe ergibt TRUE (wahr), wenn eine der Bedingungen in der Gruppe TRUE (wahr) ist.
- Die Gruppe NOT AND ergibt TRUE (wahr), wenn eine der Bedingungen in der Gruppe FALSE (falsch) ergibt.
- Die Gruppe NOT OR ergibt TRUE (wahr), wenn alle Bedingungen in der Gruppe FALSE (falsch) ergeben.

Standardmäßig ist AND der logische Operator zwischen den Bedingungen in einer Bedingungsgruppe. Es ist möglich, den logischen Operator zu ändern, indem die Bedingungsgruppe in einen anderen Gruppentyp umgewandelt wird.

Wenn Sie eine Bedingung hinzufügen, fordert Sie der Workflow Designer zunächst zur Angabe auf, was die Bedingung bewerten soll. Die folgenden Optionen sind verfügbar:

- **Eigenschaft des Arbeitsablaufzielobjekts.** Diese Option dient dazu, den Wert einer bestimmten Eigenschaft des Zielobjekts der Anfrage zu bewerten, die den Arbeitsablauf gestartet hat. Sie können die gewünschte Eigenschaft auswählen, wenn Sie eine Bedingung konfigurieren.
- **Eigenschaft des Arbeitsablaufinitiators.** Diese Option dient dazu, den Wert einer bestimmten Eigenschaft des Benutzers zu bewerten, dessen Anfrage den Arbeitsablauf gestartet hat. Sie können die gewünschte Eigenschaft auswählen, wenn Sie eine Bedingung konfigurieren.
- **Geänderter Wert der Eigenschaft des Arbeitsablaufzielobjekts.** Diese Option dient dazu, den Wert zu bewerten, dessen Zuweisung zu einer bestimmten Eigenschaft des Arbeitsablaufzielobjekts angefordert wurde, das die angeforderte Änderung an der Eigenschaft des Zielobjekts der Anfrage darstellt, die den Arbeitsablauf gestartet hat. Sie können die gewünschte Eigenschaft auswählen, wenn Sie eine Bedingung konfigurieren.

- **Arbeitsablaufparamaterwert.** Diese Option dient zur Bewertung des Werts eines bestimmten Parameters des Arbeitsablaufs. Sie können den gewünschten Parameter aus der Arbeitsablaufdefinition auswählen, wenn Sie eine Bedingung konfigurieren.
- **Eigenschaft des Objekts aus dem Arbeitsablaufdatenkontext.** Diese Option dient zur Bewertung des Werts einer bestimmten Eigenschaft des Objekts, die auf der Grundlage der Daten ausgewählt wird, die zum Zeitpunkt der Auswertung der Arbeitsablauf-Startbedingungen in der Arbeitsablaufumgebung gefunden wurden. Wenn Sie eine Bedingung konfigurieren, können Sie die gewünschte Eigenschaft auswählen und angeben, welches Objekt das Arbeitsablauf-Modul bei der Bewertung der Bedingung beim Start des Arbeitsablaufs auswählen soll.
- **Wert durch Regel-Ausdruck generiert.** Diese Option dient zur Bewertung des Zeichenkettenwerts einer bestimmten Regelausnahme. Durch die Verwendung einer Regelausnahme können Sie einen Zeichenkettenwert auf der Basis der Eigenschaften verschiedener, in der Arbeitsablaufumgebung zum Zeitpunkt der Auswertung der Arbeitsablauf-Startbedingungen gefundener Objekte zusammenstellen. Das Arbeitsablauf-Modul berechnet den Wert Ihrer Regelausnahme bei der Bewertung der Bedingung beim Start des Arbeitsablaufs.

Wenn Sie die Einheit oder das Feld angegeben haben, die bzw. das die Bedingung bewerten soll, dann können Sie einen Vergleichsoperator auswählen und einen Vergleichswert angeben. Der Vergleichsoperator legt den Vergleichsvorgang zwischen zu bewertender Einheit bzw. zu bewertendem Feld mit dem von Ihnen angegebenen Vergleichswert fest und führt abhängig vom Ergebnis dieses Vorgangs dazu, dass die Bedingung TRUE oder FALSE ergibt.

Sie können für die Festlegung eines Vergleichswerts unter den folgenden Optionen wählen:

- **Textfolge.** Führt den Vergleich mit einer Literalzeichenkette durch. Sie können die gewünschte Zeichenkette eingeben, wenn Sie eine Bedingung konfigurieren.
- **Eigenschaft des Arbeitsablaufzielobjekts.** Führt den Vergleich mit dem Wert einer bestimmten Eigenschaft des Zielobjekts der Anfrage durch, die den Arbeitsablauf gestartet hat. Sie können die gewünschte Eigenschaft auswählen, wenn Sie eine Bedingung konfigurieren.
- **Eigenschaft des Arbeitsablaufinitiators.** Führt den Vergleich mit dem Wert einer bestimmten Eigenschaft des Benutzers durch, dessen Anfrage den Arbeitsablauf gestartet hat. Sie können die gewünschte Eigenschaft auswählen, wenn Sie eine Bedingung konfigurieren.
- **Geänderter Wert der Eigenschaft des Arbeitsablaufzielobjekts.** Führt den Vergleich mit dem Wert durch, dessen Zuweisung zu einer bestimmten Eigenschaft des Arbeitsablaufzielobjekts angefordert wurde, das die angeforderte Änderung an der Eigenschaft des Zielobjekts der Anfrage darstellt, die den Arbeitsablauf gestartet hat. Sie können die gewünschte Eigenschaft auswählen, wenn Sie eine Bedingung konfigurieren.
- **Arbeitsablaufparameterwert.** Führt den Vergleich mit dem Wert eines bestimmten Parameters des Arbeitsablaufs durch. Sie können den gewünschten Parameter aus der Arbeitsablaufdefinition auswählen, wenn Sie eine Bedingung konfigurieren.
- **Eigenschaft des Objekts aus dem Arbeitsablaufdatenkontext.** Führt den Vergleich mit dem Wert einer bestimmten Eigenschaft des Objekts durch, die auf der Grundlage der Daten ausgewählt wird, die zum Zeitpunkt der Auswertung der Arbeitsablauf-Startbedingungen in der Arbeitsablaufumgebung gefunden wurden. Wenn Sie eine Bedingung konfigurieren, können Sie die gewünschte Eigenschaft auswählen und angeben, welches Objekt das Arbeitsablauf-Modul bei der Bewertung der Bedingung beim Start des Arbeitsablaufs auswählen soll.

- **Wert durch Regel-Ausdruck generiert.** Führt den Vergleich mit dem Zeichenkettenwert einer bestimmten Regelausnahme durch. Durch die Verwendung einer Regelausnahme können Sie einen Zeichenkettenwert auf der Basis der Eigenschaften verschiedener, in der Arbeitsablaufumgebung zum Zeitpunkt der Auswertung der Arbeitsablauf-Startbedingungen gefundener Objekte zusammenstellen. Das Arbeitsablauf-Modul berechnet den Wert Ihrer Regelausnahme bei der Bewertung der Bedingung beim Start des Arbeitsablaufs.

Schritte zur Konfiguration der Filterbedingungen

Das **Änderungs-Workflow-Optionen und Startbedingungen**-Dialogfeld stellt einen Bedingungsgenerator für die Konfigurierung eines für die Workflow-Startbedingungen spezifischen Filters bereit, der sich im Bereich **Filterbedingungen** im **Bedingungen**-Tab befindet. Sie erhalten Zugang zum Bedingungsgenerator in dem Felder unter der Überschrift **Workflow beginnt erst, wenn diese Bedingungen erfüllt sind**.

Wenn Sie einen Filter konfigurieren, müssen Sie mindestens eine Bedingung hinzufügen. Standardmäßig wird eine einzige implizite Bedingungsgruppe erstellt, wenn Sie eine Bedingung hinzufügen. Sie können weitere Bedingungsgruppen erstellen, um eine Reihe von Bedingungen zu gruppieren und um gruppierte Bedingungen innerhalb anderer Bedingungsgruppen zu verschachteln.

Eine Bedingungsgruppe enthält eine oder mehrere Bedingungen, die durch denselben logischen Operator miteinander verbunden sind. Durch die Gruppierung von Bedingungen geben Sie an, dass diese Bedingungen als eine Einheit bewertet werden sollen. Der Effekt ist derselbe, als wenn Sie einen Ausdruck in einer mathematischen Gleichung oder in einer logischen Aussage in Klammern setzen.

Um eine Bedingung in einer Bedingungsgruppe hinzuzufügen

- Klicken Sie im Bedingungsgenerator auf den Namen der Bedingungsgruppe und dann auf **Bedingung einfügen**.

  – ODER –

  Klicken Sie auf das Pluszeichen (+) neben dem Namen der Bedingungsgruppe.

Sie können bei Bedarf eine Bedingung entfernen, indem Sie auf das Schalt **Bedingung löschen**-Schaltfeld mit der Aufschrift **X** auf der rechten Seite des Listeneintrags klicken, der die Bedingung im Bedingungsgenerator darstellt.

Eine Bedingungsgruppe in einer anderen Bedingungsgruppe hinzufügen

- Klicken Sie auf den Namen der Bedingungsgruppe, gehen Sie auf **Bedingungsgruppe einfügen** und klicken Sie auf eine Option, um die logische Verknüpfung anzugeben.
  - **AND-Gruppe.** Die Bedingungsgruppe wertet zu TRUE aus, wenn alle Bedingungen in der Gruppe TRUE sind.
  - **OR-Gruppe.** Die Bedingungsgruppe wertet zu TRUE aus, wenn jede Bedingung in der Gruppe TRUE ist.
  - **NOT AND-Gruppe.** Die Bedingungsgruppe wertet zu TRUE aus, wenn jede Bedingung zu FALSE wertet.
  - **NOT AND-Gruppe.** Die Bedingungsgruppe wertet zu TRUE aus, wenn jede Bedingung zu FALSE wertet.

Standardmäßig ist AND der logische Operator zwischen den Bedingungen in einer Bedingungsgruppe. Es ist möglich, die logische Verknüpfung durch Konvertieren der Bedingungsgruppe in einen anderen Gruppentyp zu ändern. Klicken Sie auf den Namen der Gruppe, gehen Sie auf **Bedingungsgruppe konvertieren** und klicken Sie auf die der gewünschten logischen Verknüpfung entsprechende Option.

Sie können auch eine gesamte Bedingungsgruppe entfernen, indem Sie auf den Namen der Gruppe und dann auf **Bedingungsgruppe löschen** klicken.

Wenn Sie eine Bedingung in einer Bedingungsgruppe hinzugefügt haben, können Sie mit den folgenden Schritten die Bedingungen konfigurieren.

Eine Bedingung konfigurieren

1. Klicken Sie auf **Zu bewertende Bedingung konfigurieren** und wählen Sie unter den folgenden Optionen, um die Entität oder das Feld, die nach der Bedingung bewertet werden sollen, anzugeben:
   - Klicken Sie auf **Eigenschaft des Workflow-Zielobjekts**, um eine besondere Eigenschaft des Workflow-Zielobjekts auszuwerten. Klicken Sie dann auf Zieleigenschaft wählen.
   - Klicken Sie auf **Eigenschaft des Workflow-Initiators**, um eine besondere Eigenschaft des Workflow-Initiators auszuwerten. Klicken Sie dann auf Zieleigenschaft wählen.
   - Klicken Sie auf **Geänderter Wert der Workflow-Zielobjekt-Eigenschaft**, um die angeforderten Änderungen an einer bestimmten Eigenschaft des Workflow-Zielobjekts auszuwerten. Klicken Sie dann auf Zieleigenschaft wählen.
   - Klicken Sie auf **Workflow-Parameterwert**, um den Wert eines bestimmten Parameters des Workflow auszuwerten. Klicken Sie dann auf Gewünschten Parameter wählen.
   - Klicken Sie auf **Eigenschaft des Objekts aus dem Workflow-Datenkontext**, um eine bestimmte Eigenschafts eines bestimmten am Workflow beteiligten Objekts auszuwerten. Klicken Sie dann auf Zielobjekt und Zieleigenschaft wählen.
   - Klicken Sie auf **Durch Regelausdruck generierter Wert**, um den von einem bestimmten Regelausdruck generierten Zeichenfolgewert auszuwerten. Klicken Sie dann auf Einträge zum Regelausdruck hinzufügen.
2. Klick Sie bei Bedarf auf den aktuellen Vergleichsoperator und dann auf den Operator, den die Bedingung verwenden soll.

   *Standardmäßig wird eine Bedingung für die Verwendung des **Ist gleich**-Operators konfiguriert.*
3. Klicken Sie auf **Vergleichswert definieren** und wählen Sie aus den folgenden Optionen, um den gewünschten Vergleichswert anzugeben:
   - Klicken Sie auf **Textzeichenfolge**, um den Vergleich mit einer literalen Zeichenfolge durchzuführen. Geben Sie dann die gewünschte Folge ein.
   - Klicken Sie auf **Eigenschaft des Workflow-Zielobjekts**, um den Vergleich mit dem Wert einer besonderen Eigenschaft des Workflow-Zielobjekts durchzuführen. Klicken Sie dann auf Zieleigenschaft wählen.
   - Klicken Sie auf **Eigenschaft des Workflow-Initiators**, um den Vergleich mit dem Wert einer besonderen Eigenschaft des Workflow-Initiators durchzuführen. Klicken Sie dann auf Zieleigenschaft wählen.
   - Klicken Sie auf **Geänderter Wert der Workflow-Zielobjekteigenschaft**, um den Vergleich mit dem Wert, der angefordert wird, um einer bestimmten Eigenschaft des Workflow-Zielobjekts zugeteilt zu werden, durchzuführen. Klicken Sie dann auf Zieleigenschaft wählen.

- Klicken Sie auf **Workflow-Parameterwert**, um den Vergleich mit dem Wert eines bestimmten Parameters des Workflow durchzuführen. Klicken Sie dann auf Gewünschten Parameter wählen.
- Klicken Sie auf **Eigenschaft des Objekts aus dem Workflow-Datenkontext**, um den Vergleich mit dem Wert einer bestimmten Eigenschafts eines bestimmten am Workflow beteiligten Objekts durchzuführen. Klicken Sie dann auf Zielobjekt und Zieleigenschaft wählen.
- Klicken Sie auf **Durch Regelausdruck generierter Wert**, um den Vergleich mit dem von einem bestimmten Regelausdruck generierten Zeichenfolgewert durchzuführen. Klicken Sie dann auf Einträge zum Regelausdruck hinzufügen.

Konfiguration der skriptbasierten Bedingungen

Um eine skriptbasierte Bedingung zu konfigurieren, müssen Sie ein Skriptmodul erstellen und anwenden, das eine Funktion enthält, welche den angeforderten Vorgang analysiert, um zu bestimmten, ob der Workflow beginnen kann. Die Funktion kann den ActiveRoles-ADSI-Provider verwenden, um auf die Eigenschaften von Objekten zuzugreifen, die am Vorgang beteiligt sind, die Eigenschaften analysieren und je nach dem Ergebnis der Analyse TRUE oder FALSE zurückgeben. Der Arbeitsablauf startet, wenn die Funktion TRUE ausgibt.

Gehen Sie folgendermaßen vor, um die skriptbasierte Bedingung anzuwenden:

1. Klicken Sie im Bedingungsgenerator auf den Namen der Bedingungsgruppe und dann auf **Bedingung einfügen**.
2. Klicken Sie auf **Auszuwertende Bedingung konfigurieren** und dann auf **Durch Regelausdruck generierter Wert**.
3. Klicken Sie im Dialogfeld **Regelausdruck konfigurieren** auf **Eingabe hinzufügen** und dann auf **Durch Skript generierter Wert**.
4. Wählen Sie im Dialogfeld **Eingabe konfigurieren** das entsprechende Skriptmodul und die entsprechende Skriptfunktion.
5. Klicken Sie auf **OK**, um das Dialogfeld **Eingabe konfigurieren** zu schließen.
6. Klicken Sie auf **OK**, um das Dialogfeld **Regelausdruck konfigurieren** zu schließen.
7. Überprüfen Sie im Bedingungsgenerator, ob der Vergleichsoperator **Ist gleich** gewählt wurde.
8. Klicken Sie auf **Vergleichswert definieren** und dann auf **Textfolge**.
9. Geben Sie im Dialogfeld **Eingabe konfigurieren** unter **Textfolge** TRUE ein.
10. Klicken Sie auf **OK**, um das Dialogfeld **Eingabe konfigurieren** zu schließen.
11. Klicken Sie auf **OK** um das Dialogfeld **Workflow-Optionen und Startbedingungen ändern** zu schließen.
12. Speichern Sie ihre Änderungen an der Arbeitsablaufdefinition.

Nach Ausführung dieser Schritte setzt der Workflow ein, wenn die in Schritt 4 angegebene Funktion nach der Auswertung der Bedingung zum Zeitpunkt des Workflow-Starts TRUE zurückgibt.

Weitere Informationen und Anweisungen erhalten Sie unter „Entwicklung von Skriptbedingungsfunktionen" in Quest One ActiveRoles SDK.

Optionen „Ausführen als"

Die Option „Ausführen als" legt das Benutzerkonto fest, unter dem der Arbeitsablauf ausgeführt wird. Klicken Sie auf die Verknüpfung **Optionen für „Ausführen als"** auf der Seite **Optionen und Startbedingungen des Arbeitsablaufs**, um die Kontoeinstellungen anzuzeigen bzw. zu ändern. Sie können unter den folgenden Optionen wählen:

- **Das Dienstkonto von Quest One ActiveRoles.** Der Arbeitsablauf wird unter dem Konto des Verwaltungsdienstes ausgeführt, der für den Start des Arbeitsablaufs auf Aufforderung verwendet wurde.
- **Konto des Benutzers, der den Arbeitsablauf gestartet hat.** Der Arbeitsablauf wird unter dem Windows-Konto des Benutzers ausgeführt, der den Vorgang angefordert hat, der den Arbeitsablauf gestartet hat.

Alle Aktivitäten innerhalb des Arbeitsablaufs werden normalerweise unter dem Konto ausgeführt, das von der Option „Ausführen als" für den Arbeitsablauf angegeben ist. Jede Aktivität kann jedoch so konfiguriert werden, dass Sie individuelle Optionen für „Ausführen als" verwendet. Die Eigenschaftsseite für die Aktivität enthält die Verknüpfung **Optionen für „Ausführen als"**, die es Ihnen ermöglicht, die Arbeitsablaufeinstellung „Ausführen als" auf der Basis der einzelnen Aktivitäten zu übergehen.

Bei Ausführung unter dem Konto des Verwaltungsdienstes haben die Arbeitsablaufaktivitäten dieselben Rechte und Berechtigungen wie der Verwaltungsdienst selbst und können somit jegliche Aufgaben ausführen, die für den Verwaltungsdienst zulässig sind.

Bei Ausführung unter dem Konto des Benutzers, der den Arbeitsablauf gestartet hat, können die Aktivitäten nur die Aufgaben durchführen, die Quest One ActiveRoles für dieses Benutzerkonto zulässt. Der Verwaltungsdienst verarbeitet die Aktivitäts-Vorgangsanforderung, als wenn diese von diesem Benutzer über eine ActiveRoles Benutzeroberfläche gesendet wurden, so dass die Aktivitäten über die Rechte und Berechtigungen verfügen, die dem Benutzerkonto in Quest One ActiveRoles gewährt wurden.

Genehmigung erzwingen

Die Option **Genehmigung erzwingen** legt fest, ob Genehmigungsregeln auf die vom Änderungen angewandt werden sollen, die von dem Arbeitsablauf angefordert wurden, der unter einem privilegierten Konto ausgeführt wird. Durch diese Auswahl dieser Option können die von den Aktivitäten „Arbeitsablauf" angeforderten Änderungen, deren Genehmigung noch aussteht, unabhängig von dem Konto, unter welchem der Arbeitsablauf ausgeführt wird, zur Genehmigung eingereicht werden. Andernfalls werden die Änderungen angewandt, ohne die Genehmigung abzuwarten, wenn der Arbeitsablauf unter dem Dienstkonto von Quest One ActiveRoles, dem Konto der genehmigenden Instanz oder des Quest One ActiveRoles-Verwalters ausgeführt wird. Diese Option kann je nach Aktivität überschrieben werden.

Workflow-Parameter konfigurieren

Arbeitsablaufparameter dienen zur Weitergabe ihrer Werte bei Ausführung an die Arbeitsablaufaktivitäten. Sie können Parameterwerte angeben, wenn Sie einen Arbeitsablauf konfigurieren. In diesem Fall speichert ActiveRoles die Parameterwerte als Teil der Arbeitsablaufdefinition und fragt sie dann bei Bedarf bei Ausführung des Arbeitsablaufs ab. Eine weitere Option ist die Verwendung eines Skripts für die Generierung des Werts eines Arbeitsablaufparameters bei Ausführung.

Sie können Parameter verwenden, um die Wiederverwendbarkeit eines Arbeitsablaufs zu erhöhen. Wenn beispielsweise ein Wert in der Konfiguration einer Arbeitsablaufaktivität angegeben ist, dann müssen Sie diese Aktivität neu konfigurieren, wenn Sie den Wert ändern möchten. Mit Arbeitsablaufparametern können Sie die vorhandene Konfiguration der Aktivität wiederverwenden, indem Sie den entsprechenden Wert über einen Parameter weitergeben. Nachfolgend sind einige Beispiele für die Nutzung von Arbeitsablaufparametern aufgeführt:

- **Arbeitsablauf-Startbedingungen.** Wenn Sie Arbeitsablauf-Startbedingungen konfigurieren, können Sie einen Filter erstellen, der dazu führt, dass der Arbeitsablauf startet, wenn die Eigenschaften der Vorgangsanforderung mit dem Wert eines bestimmten Parameters übereinstimmen.
- **Wenn-Dann-Sonst-Zweigbedingungen.** Wenn Sie Bedingungen für einen Wenn-Dann-Sonst-Zweig konfigurieren, können Sie eine Bedingung einrichten, die dazu führt, dass der Arbeitsablauf diesen Zweig wählt, wenn ein bestimmter Parameter einen bestimmten Wert aufweist.
- **Container durchsuchen.** Wenn Sie eine Suchaktivität konfigurieren, können Sie diese Option auswählen, die dazu führt, dass die Aktivität in der Organisationseinheit oder in dem Container sucht, der durch den Wert eines bestimmten Parameters angegeben wird.
- **Suchfilter.** Wenn Sie eine Suchaktivität konfigurieren, können Sie eine Suchfilterbedingung einrichten, die dazu führt, dass die Aktivität nach Objekten sucht, deren Eigenschaften mit dem Wert eines bestimmten Parameters übereinstimmen.
- **Erstellungscontainer.** Sie können eine Aktivität des Typs „Erstellen" mit der Option zur Erstellung von Objekten in der Organisationseinheit oder in dem Container konfigurieren, die bzw. der vom Wert eines bestimmten Parameters angegeben wird.
- **Einrichten von Objekteigenschaften.** Sie können eine Aktivität des Typs „Erstellen" oder „Aktualisieren" mit der Option zum Festlegen oder Ändern der Eigenschaften des Objekts auf der Grundlage des Werts eines bestimmten Parameters konfigurieren.
- **Auswählen eines Zielobjekts.** Sie können eine Aktivität konfigurieren, um Änderungen an dem Objekt durchzuführen, das durch den Wert eines bestimmten Parameters angegeben wird. Dies gilt für Aktivitäten, die zum Ziel haben, Änderungen an Objekten in Active Directory vorzunehmen (wie etwa die Aktivität „Aktualisieren", „Zu Gruppe hinzufügen", „Verschieben" etc.
- **Zielcontainer.** Sie können eine Aktivität des Typs „Verschieben" konfigurieren, um das Objekt in die Organisationseinheit oder in den Container zu verschieben, die bzw. der vom Wert eines bestimmten Parameters angegeben wird.

Jeder Parameter verfügt über eine Reihe von Eigenschaften, die den Parameter definieren. Hierzu zählen unter anderem folgende Eigenschaften:

- **Name.** Jeder Parameter muss über einen eindeutigen Namen in der Arbeitsablaufdefinition verfügen.
- **Description.** Sie können diese Eigenschaft verwenden, um dem Zweck des Parameters zu beschreiben.

- **Display name.** Diese Eigenschaft gibt den benutzerfreundlichen Namen des Parameters an.
- **Syntax.** Diese Eigenschaft legt den Datentyp des Parameterwerts fest.
  - **String.** Diese Syntax gibt an, dass der Parameterwert eine Zeichenfolge ist. Sie können die Zeichenfolge eingeben, wenn Sie den Wert des Parameters festlegen.
  - **DateTime.** Diese Syntax gibt an, dass der Parameter ein Datums- und Zeitwert speichert. Sie können die Datums- und Uhrzeitauswahl verwenden, um den Parameterwert anzugeben.
  - **DN.** Diese Syntax gibt an, dass der Parameterwert der eindeutige Name (Distinguished Name) eines bestimmten Objekts ist. Sie können die Objektauswahl verwenden, um den Parameterwert anzugeben.
  - **ObjectGUID.** Diese Syntax gibt an, dass der Parameterwert der globale eindeutige Kennzeichner (Globally Unique Identifier (GUID)) eines bestimmten Objekts ist. Sie können die Objektauswahl verwenden, um den Parameterwert anzugeben.
  - **SID.** Diese Syntax gibt an, dass der Parameterwert die Sicherheits-ID (SID) eines bestimmten Objekts ist. Sie können die Objektauswahl verwenden, um den Parameterwert anzugeben.
  - **SecureString.** Diese Syntax gibt an, dass die Arbeitsablaufdefinition den Parameterwert in verschlüsselter Form unter Verwendung eines vom ActiveRoles-Dienst bereitgestellten Verschlüsselungscodes speichert. Sie können diese Syntax verwenden, um sensitive Daten wie etwa Passwörter zu handhaben.
  - **AttributeName.** Diese Syntax gibt an, dass der Parameterwert der Name eines bestimmten Attributs aus dem Verzeichnisschema ist. Sie können die Attributauswahl verwenden, um den Parameterwert anzugeben.
- **Number of values.** Standardmäßig kann ein Parameter einen einzigen Wert speichern. Sie können einen Parameter so konfigurieren, dass er mehrere Werte speichert.
- **Value is required.** Standardmäßig muss ein Parameter keinen Wert haben. Sie können einen Parameter so konfigurieren, dass der Workflow Designer die Speicherung der Arbeitsablaufdefinition nicht zulässt, wenn diesem Parameter kein Wert zugewiesen ist.
- **List of acceptable values.** Diese Eigenschaft gibt eine Liste der zulässigen Werte an, die dem Attribut zugewiesen werden können. Wenn ein bestimmter Parameter diese Eigenschaft aufweist, dann erfordert der Workflow Designer, dass der Wert für diesen Parameter aus der Liste stammt, wenn Sie den Parameterwert angeben. Wenn Sie einen Parameter konfigurieren, können Sie explizit eine Liste angeben oder Sie können den Parameter so konfigurieren, dass er ein Skript verwendet, das bei Ausführung des Arbeitsablaufs eine Liste der zulässigen Werte oder einen einzelnen Wert für diesen Parameter generiert.

Hinzufügung eines Parameters zu einer Workflow-Definition

1. Erweitern Sie in der Quest One ActiveRoles-Konsolenstruktur **Konfiguration | Richtlinien | Workflow** und wählen Sie den Workflow, den Sie konfigurieren möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.

2. Klicken Sie im Bereich „Details" auf die Schaltfläche **Optionen und Startbedingungen des Arbeitsablaufs**, um den Bereich über dem Prozessdiagramm zu erweitern, und klicken Sie dann auf die Schaltfläche **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Parameter** in dem sich öffnenden Dialogfeld.
4. Klicken Sie auf der **Parameter**-Seite auf **Hinzufügen**, um das Dialogfeld **Parameterdefinition** zu öffnen.

5. Füllen Sie im Dialogfeld **Parameterdefinition** die folgenden Felder aus:
   - **Name.** Geben Sie hier den Namen ein, den Sie dem Parameter geben wollen. Der Name darf in der Workflow-Definition nur einmal vorkommen.
   - **Beschreibung.** Geben Sie hier eine Beschreibung des Parameters ein. Dieses Feld ist optional.
   - **Angezeigter Name.** Geben Sie hier den benutzerfreundlichen Namen ein, den Sie dem Parameter geben wollen.
   - **Syntax.** Wählen Sie in dieser Liste die Syntax, die Sie dem Parameter geben wollen. Siehe die Liste der Syntaxoptionen weiter oben.

     Wenn Sie die Syntaxoption **AttributeName** wählen, werden Sie aufgefordert, die Attributauswahl für diesen Parameter zu konfigurieren. Wählen Sie die Objektklasse, deren Attribute standardmäßig in der Attributwahl aufgeführt werden sollen, und geben Sie an, ob der Attributwähler eine andere Objektklasse wählen darf. Sie können außerdem angeben, ob der Attributwähler ein einziges Attribut oder mehrere Attribute wählen darf.
6. Wenn Sie möchten, dass der Parameter eine Sammlung mehrerer Werte speichert, wählen Sie das Kontrollkästchen **Dieser Parameter ist mehrwertig**.
7. Wenn Sie wollen, dass der Workflow-Designer voraussetzt, dass dem Parameter ein Wert zugeordnet wird, wählen Sie das Kontrollkästchen **Dieser Parameter muss einen Wert haben**.
8. Wenn Sie eine Liste der für den Parameter akzeptablen Werte angeben möchten, gehen Sie wie folgt vor:
   - Konfigurieren Sie eine explizite Liste von Werten mit Hilfe der Schaltflächen **Hinzufügen**, **Ändern** und **Entfernen** unter dem Kästchen **Akzeptable Werte**.
   - Klicken Sie auf **Skript zur Bestimmung der Parameterwerte verwenden** unter dem Kästchen **Akzeptable Werte**, wenn Sie wollen, dass während der Laufzeit des Workflow eine Liste akzeptabler Werte von einem Skript generiert werden soll. Klicken Sie dann auf die Schaltfläche naben dem Kästchen **Skriptname**, um das Skriptmodul zu wählen, das das gewünschte Skript enthält. Das Skriptmodul muss zuvor erstellt werden. Wenn Sie ein Skriptmodul ausgewählt haben, klicken Sie in der Liste **Funktion, um eine Liste akzeptabler Werte zu definieren** auf den Namen der Skriptfunktion. Sie können aus den Skriptfunktionen im Skriptmodul wählen. Die Funktion muss so konstruiert sein, dass sie eine Sammlung von Werten ergibt, die der Syntax des Parameters entsprechen.
9. Wenn Sie ein Skript verwenden möchten, um dem Parameter bei der Ausführung des Arbeitsablaufs einen Wert zuzuweisen, klicken Sie auf **Das Skript verwenden, um die Parameter festzulegen** unter dem Feld **Akzeptable Werte**. Klicken Sie dann auf die Schaltfläche neben dem Kästchen **Skriptname**, um das Skriptmodul zu wählen, das das gewünschte Skript enthält. Das Skriptmodul muss zuvor erstellt werden. Wenn Sie ein Skriptmodul ausgewählt haben, klicken Sie in der Liste **Funktion, um diesem Parameter einen Wert zuzuweisen** auf den Namen der Skriptfunktion. Sie können aus den Skriptfunktionen im Skriptmodul wählen. Die Funktion muss so konstruiert sein, dass sie einen Wert ergibt, der der Syntax des Parameters entspricht.

Mit Parametern werden beim Konfigurieren oder Starten des Arbeitsablaufs bestimmte Daten angegeben; wenn der Arbeitsablauf läuft, werden diese Daten an Aktivitäten „Arbeitsablauf" übergeben. Die Daten werden als Parameterwerte dargestellt. Zum Zuordnen eines Wertes zu einem vorgegebenen Parameter wählen Sie den Parameter aus der Liste auf der Registerkarte **Parameter** und klicken Sie auf die Schaltfläche **Parameterwert anzeigen oder ändern**.

Hinzufügen von Aktivitäten zu einem Arbeitsablauf

Die Quest One ActiveRoles-Konsole stellt den Workflow-Designer für die Erstellung und Konfiguration der Workflows bereit. Zunächst erstellen Sie eine Arbeitsablaufdefinition. Verwenden Sie dann den Workflow Designer, um den Arbeitsablauf durch Hinzufügen und Konfigurieren von Arbeitsablaufaktivitäten zu erstellen.

Gehen Sie folgendermaßen vor, um eine Aktivität zu einem Arbeitsablauf hinzuzufügen:

1. Erweitern Sie in der Quest One ActiveRoles-Konsolenstruktur **Konfiguration | Richtlinien | Workflow** und wählen Sie den Workflow, in welchem Sie eine Aktivität hinzufügen möchten.
   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.
2. Ziehen Sie im Bereich „Details" die Aktivität vom linken Bereich auf das Prozessdiagramm.
3. Klicken Sie mit der rechten Maustaste auf den Namen der Aktivität im Prozessdiagramm und klicken Sie dann auf **Eigenschaften**.
4. Verwenden Sie das Dialogfeld **Eigenschaften**, um die Aktivität zu konfigurieren. Die Anweisungen sind weiter unten in diesem Kapitel aufgeführt.

Wenn Sie eine Aktivität zum oberen Teil des Diagramms hinzufügen (über der Zeile **Vorgangsausführung**), dann wird die Aktivität in der Vorausführungsphase der Vorgangsverarbeitung ausgeführt (siehe „Übersicht über den Arbeitsablaufprozess" weiter oben in diesem Kapitel). Wenn Sie eine Aktivität zum unteren Teil des Diagramms hinzufügen (unter der Zeile **Vorgangsausführung**), dann wird die Aktivität in der Nachausführungsphase der Vorgangsverarbeitung ausgeführt. Bestimmte Aktivitäten wie etwa eine Genehmigungsaktivität, die für eine Aufführung in der Vorausführungsphase konzipiert sind, können nicht zum unteren Teil des Diagramms hinzugefügt werden.

Im Dialogfeld **Eigenschaften** können Sie den Namen und die Beschreibung der Aktivität ändern. Diese Einstellungen gelten für alle Aktivitäten. Der Name gibt die Aktivität im Prozessdiagramm an. Die Beschreibung wird als QuickInfo angezeigt, wenn Sie auf die entsprechende Aktivität im Prozessdiagramm zeigen. Um eine Aktivität aus dem Prozessdiagramm zu entfernen, klicken Sie mit der rechten Maustaste auf den Namen der Aktivität und klicken Sie dann auf **Löschen**.

Konfigurieren einer Genehmigungsaktivität

Die Aufgabe der Konfigurierung einer Genehmigungsaktivität besteht aus folgenden Schritten:

- **Die genehmigenden Instanzen wählen und die Eskalation konfigurieren.** Sie müssen mindestens eine Liste genehmigender Instanzen für die erste Ebene der genehmigenden Instanz wählen. Quest One ActiveRoles weist zuerst Genehmigungsaufgaben den genehmigenden Instanzen auf dieser Ebene zu. Sie können zum Aktivieren der Eskalation von Genehmigungsaufgaben weitere Ebenen von genehmigenden Instanzen konfigurieren.
- **Die Eigenschaften, die die genehmigenden Instanz prüfen, angeben oder ändern soll, wählen.** Sie können die Objekteigenschaften auflisten, die die genehmigende Instanz bei der Ausführung einer Genehmigungsaufgabe bereitstellen muss (Anfrage nach weiteren Informationen) und festlegen, ob die genehmigende Instanz die für Genehmigung eingereichten Objekteigenschaften sehen oder ändern darf (Anfrage nach Überprüfung).
- **Die Seiten für die Ausführung der Genehmigungsaufgabe konfigurieren.** Sie können die Kopfzeile der Seite für die Genehmigungsaufgabe konfigurieren, indem Sie den Aufgabentitel und die Objekteigenschaften auswählen, die in diese Kopfzeile aufgenommen werden sollen, und benutzerdefinierte interaktive Schaltflächen neben den standardmäßigen Schaltflächen **Genehmigen** und **Ablehnen** erstellen.

- **Die Benachrichtigung konfigurieren.** Sie können die Arbeitsablaufereignisse wählen, für die eine Benachrichtigung ergehen soll, die Empfänger der Benachrichtigung angeben und die Benachrichtigungsmeldung selbst anpassen.

Dieser Abschnitt enthält eine Anleitung:

- Konfigurieren der genehmigenden Instanzen
- Konfigurieren der Eskalation
- Konfiguration der Anfrage nach weiteren Informationen
- Konfiguration der Anfrage nach Prüfung
- Anpassen des Kopfes der Genehmigungsaufgaben-Seite
- Anpassung der Aktionsschaltflächen für Genehmigung

Anweisungen bezüglich der Konfiguration von Benachrichtigungseinstellungen finden Sie unter Konfigurieren einer Benachrichtigungsaktivität weiter unten in diesem Dokument.

Konfigurieren der genehmigenden Instanzen

Damit eine Genehmigungsrichtlinie gültig ist, muss mindestens eine Liste der Genehmiger für die erste Genehmigungsebene angegeben werden. Quest One ActiveRoles weist die Genehmigungsaufgabe zunächst dem Genehmiger dieser Ebene zu. Sie können zum Aktivieren der Eskalation von Genehmigungsaufgaben weitere Ebenen von genehmigenden Instanzen konfigurieren.

Gehen Sie zum Angeben von genehmigenden Instanzen für die erste Ebene „Genehmigende Instanzen" wie folgt vor:

1. Erweitern Sie in der Konsolenstruktur Quest One ActiveRoles **Konfiguration | Richtlinien | Arbeitsablauf** und wählen Sie dann den Arbeitsablauf, der die Genehmigungsaktivität enthält, die Sie konfigurieren möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.
2. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Genehmigungsaktivität und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie im Dialogfeld **Eigenschaften** auf die Registerkarte **Genehmigende Instanzen**.
4. Überprüfen Sie, ob die Option **Erste genehmigende Instanz - Ebene 0** im Feld **Die zu konfigurierende Ebene der genehmigenden Instanz wählen** ausgewählt ist.
5. Klicken Sie auf die Schaltfläche **Genehmigende Instanzen festlegen**.
6. Aktivieren Sie auf der Seite **Auswahl der genehmigenden Instanzen** die entsprechenden Kontrollkästchen, um genehmigende Instanzen festzulegen.
7. Wenn Sie **Diese Benutzer oder Gruppen** aktiviert haben, verwenden Sie die Schaltflächen **Hinzufügen** und **Entfernen**, um die Liste der genehmigenden Instanzen zu konfigurieren.

Wenn Sie Eskalation auf der ersten Ebene der genehmigenden Instanzen aktivieren (siehe Konfigurieren der Eskalation), müssen Sie genehmigende Instanzen für Eskalationsebene 1 angeben (die Ebene nach der ersten Ebene). Quest One ActiveRoles erlaubt bis zu 10 Ebenen mit einer Liste genehmigender Instanzen pro Ebene. Wenn Sie Eskalation auf einer bestimmten Eskalationsebene aktivieren, müssen Sie genehmigende Instanzen für die nachfolgende Ebene angeben.

Gehen Sie zum Festlegen genehmigender Instanzen für eine bestimmte Eskalationsebene wie folgt vor:

1. Klicken Sie in der Liste **Die zu konfigurierende Ebene der genehmigenden Instanz wählen** auf die zu konfigurierende Eskalationsebene.

   Zum Konfigurieren einer bestimmten Eskalationsebene müssen Sie zunächst genehmigende Instanzen angeben und Eskalation auf der darunter liegenden Ebene der genehmigenden Instanz aktivieren.

2. Klicken Sie auf die Schaltfläche **Genehmigende Instanzen festlegen**.
3. Aktivieren Sie auf der Seite **Auswahl der genehmigenden Instanzen** die entsprechenden Kontrollkästchen, um genehmigende Instanzen festzulegen.
4. Wenn Sie **Diese Benutzer oder Gruppen** aktiviert haben, verwenden Sie die Schaltflächen **Hinzufügen** und **Entfernen**, um die Liste der genehmigenden Instanzen zu konfigurieren.

Die Auswahl der genehmigenden Instanzen kann auf der Eigenschaft „Vorgesetzter" oder „Verwaltet von" basieren:

- Durch Aktivierung des Kontrollkästchens **Vorgesetzter der Person, die den Vorgang angefordert hat** konfigurieren Sie die Genehmigungsaktivität, sodass die von einem bestimmten Benutzer angeforderten Vorgänge die Genehmigung vom Vorgesetzten dieses Benutzers erfordern. Bei Auswahl dieser Option sendet der vom Benutzer initiierte Vorgang die Genehmigungsaufgabe an die als Vorgesetzten des Benutzers im Verzeichnis angegebene Person.
- Durch Aktivierung des Kontrollkästchens **Verwalter des Zielobjekts des Vorgangs** oder **Verwalter der Organisationseinheit, in dem sich das Zielobjekt des Vorgangs befindet** konfigurieren Sie die Genehmigungsaktivität, sodass die an einem bestimmten Objekt vorgenommenen Änderungen die Genehmigung vom Vorgesetzten dieses Objekts oder vom Vorgesetzten der Organisationseinheit, die dieses Objekt enthält, erfordern. Bei Auswahl dieser Optionen sendet der Vorgang, der Änderungen an einem bestimmten Objekt fordert, die Genehmigungsaufgabe an die als Vorgesetzten des Objekts oder der Organisationseinheit in dem Verzeichnis angegebene Person.
- Durch Aktivierung des Kontrollkästchens **Sekundäre Besitzer des Zielobjekts des Vorgangs** konfigurieren Sie die Genehmigungsaktivität, sodass die am Zielobjekt des Vorgangs vorgenommenen Änderungen die Genehmigung von einer beliebigen Person erfordern, die als sekundärer Besitzer dieses Objekts festgelegt wurden. Zusätzlich zum Vorgesetzten (primärer Besitzer) können sekundäre Besitzer einem Objekt zugewiesen werden, um die Arbeitslast der Objektverwaltung aufzuteilen.
- Durch Aktivierung des Kontrollkästchens **Verwalter der zur Zielgruppe hinzuzufügenden oder aus ihr zu entfernenden Person** konfigurieren Sie die Genehmigungsaktivität, sodass das Hinzufügen oder Entfernen eines Objekts zur bzw. aus der Zielgruppe des Vorgangs die Genehmigung vom Vorgesetzten dieses Objekts erfordern. Bei einer Anforderung zum Hinzufügen eines Benutzers zur Zielgruppe des Vorgangs etwa führt diese Option dazu, dass die Genehmigungsaktivität die Genehmigungsaufgabe an die Person sendet, die als der Vorgesetzte des Benutzers im Verzeichnis angegeben ist.

Wenn Sie genehmigende Instanzen für eine Eskalationsebene angeben, sind weitere Optionen verfügbar:

- **Verwalter der genehmigenden Instanz der vorigen Ebene.** Mit dieser Option eskalieren Sie die Genehmigungsaufgabe des Verwalters des Benutzers oder der Gruppe, der/die auf der darunter liegenden Ebene der genehmigenden Instanz als genehmigende Instanz festgelegt wurde. Beispiel: Ein bestimmter Benutzer ist erste genehmigende Instanz und Eskalation ist auf der ersten Ebene der genehmigenden Instanz aktiviert. Bei der Eskalation wird die Genehmigungsaufgabe dem Verwalter dieses Benutzers zugewiesen.
- **Sekundärer Besitzer der genehmigenden Instanz der vorigen Ebene.** Mit dieser Option eskalieren Sie die Genehmigungsaufgabe des sekundären Besitzers des Benutzers oder der Gruppe, der/die auf der darunter liegenden Ebene der genehmigenden Instanz als genehmigende Instanz festgelegt wurde. Beispiel: Eine bestimmte Gruppe ist erste genehmigende Instanz und Eskalation ist auf der ersten Ebene der genehmigenden Instanz aktiviert. Bei der Eskalation wird die Genehmigungsaufgabe dem sekundären Besitzer dieser Gruppe zugewiesen.

Die Auswahl von genehmigenden Instanzen kann auf einer Skriptfunktion basieren, die die genehmigende Instanz auswählt, wenn die Genehmigungsaktivität ausgeführt wird. Die Funktion kann den ADSI-Provider von Quest One ActiveRoles verwenden, um auf die Eigenschaften der am Vorgang beteiligten Objekte zuzugreifen, um die Eigenschaften zu analysieren und um eine Kennung des Benutzers oder der Gruppe auszugeben, die als genehmigende Instanz ausgewählt werden soll. Weitere Informationen und Anweisungen finden Sie im Abschnitt „Entwickeln von Funktionen für die Festlegung von genehmigenden Instanzen" in Quest One ActiveRoles SDK.

Konfigurieren der Eskalation

Eine Genehmigungsaktivität kann mehrere Ebenen genehmigender Instanzen definieren, wobei jede Ebene eine eigene Liste genehmigender Instanzen enthält. Quest One ActiveRoles nutzt Ebenen genehmigender Instanzen bei der Eskalation zeitlich begrenzter Genehmigungsaufgaben. Die Genehmigungsaktivität kann für jede Ebene genehmigender Instanzen eine bestimmte Frist angeben. Wenn eine genehmigende Instanz auf einer bestimmten Ebene die Genehmigungsaufgabe nicht innerhalb der angegebenen Frist abschließt, weist Quest One ActiveRoles die Aufgabe den genehmigenden Instanzen der nächsten Ebene zu. Dieser Prozess wird als *Eskalation* bezeichnet.

Eine gültige Genehmigungsaktivität muss eine Liste genehmigender Instanzen für die erste Ebene genehmigender Instanzen angeben. Quest One ActiveRoles weist die Genehmigungsaufgabe zunächst den genehmigenden Instanzen dieser Ebene zu. Zum Aktivieren der Eskalation muss für die nachfolgende Eskalationsebene eine eigene Liste mit genehmigenden Instanzen angegeben werden.

Zum Konfigurieren der Eskalation auf der ersten Ebene der genehmigenden Instanzen gehen Sie wie folgt vor:

1. Geben Sie genehmigende Instanzen für die erste Ebene der genehmigenden Instanzen an (Anweisungen hierzu finden Sie unter Konfigurieren der genehmigenden Instanzen weiter vorne in diesem Dokument).
2. Überprüfen Sie, ob die Option **Erste genehmigende Instanz - Ebene 0** im Feld **Die zu konfigurierende Ebene der genehmigenden Instanz wählen** ausgewählt ist.
3. Wählen Sie eine oder beide der folgenden Optionen aus:
   - **Die Genehmigungsaufgabe hat eine Frist von** <*Zahl*> **Tagen** <*Zahl*> **Stunden.** Hiermit legen Sie die Frist fest, innerhalb derer die erste genehmigende Instanz die Genehmigungsaufgabe abzuschließen hat.
   - **Zulassen, dass die genehmigende Instanz die Genehmigungsaufgabe eskaliert.** Ist diese Option ausgewählt, können die genehmigenden Instanzen der ersten Ebene ihre Genehmigungsaufgaben an die genehmigenden Instanzen von Eskalationsebene 1 übertragen.

4. Wenn Sie nur die erste Option (eine Frist für die Aufgabe) gewählt haben, wählen Sie **Genehmigungsaufgabe auf Eskalationsebene 1 eskalieren**. Andernfalls ist die Eskalation nicht aktiviert.
5. Klicken Sie im Feld **Die zu konfigurierende Ebene der genehmigenden Instanz wählen** auf **Eskalationsebene 1**.
6. Geben Sie genehmigende Instanzen für Eskalationsebene 1 an (Anweisungen hierzu finden Sie unter Konfigurieren der genehmigenden Instanzen weiter vorne in diesem Dokument).

Quest One ActiveRoles ermöglicht bis zu 10 Eskalationsebenen, wobei jede Ebene eine eigene Liste mit genehmigenden Instanzen enthält. Sie können nacheinander Eskalationsebenen konfigurieren und dadurch eine Eskalationskette erstellen. Dies bedeutet: Wenn Sie Eskalation auf der ersten Ebene der genehmigenden Instanzen konfiguriert haben, können Sie Eskalation auf Eskalationsebene 1, danach auf Ebene 2 usw. konfigurieren. Dadurch können Sie folgende Ereignisfolge erzielen. Wenn die ersten genehmigenden Instanzen die Genehmigungsaufgabe nicht rechtzeitig durchführen, wird die Aufgabe den genehmigenden Instanzen auf Eskalationsebene 1 zugewiesen. Wenn diese die Genehmigungsaufgabe nicht in der für sie geltenden Frist durchführen, wird die Aufgabe mit einer neuen Frist den genehmigenden Instanzen auf Eskalationsebene 2 zugewiesen. Diese Eskalationskette kann bis zu 10 Eskalationsebenen enthalten.

Gehen Sie zum Konfigurieren der Eskalation auf einer bestimmten Eskalationsebene wie folgt vor:

1. Klicken Sie in der Liste **Die zu konfigurierende Ebene der genehmigenden Instanz wählen** auf die zu konfigurierende Eskalationsebene.

   Zum Konfigurieren einer bestimmten Eskalationsebene müssen Sie zunächst genehmigende Instanzen angeben und Eskalation auf der darunter liegenden Ebene der genehmigenden Instanz aktivieren.

2. Wählen Sie eine oder beide der folgenden Optionen aus:
   - **Die Genehmigungsaufgabe hat eine Frist von** <*Zahl*> **Tagen** <*Zahl*> **Stunden.** Hiermit legen Sie die Frist fest, innerhalb derer die erste genehmigende Instanz die Genehmigungsaufgabe abzuschließen hat.
   - **Zulassen, dass die genehmigende Instanz die Genehmigungsaufgabe eskaliert.** Ist diese Option ausgewählt, können die genehmigenden Instanzen der aktuellen Ebene ihre Genehmigungsaufgaben an die genehmigenden Instanzen der nächsten Ebene übertragen.
3. Wenn Sie nur die erste Option (eine Frist für die Aufgabe) gewählt haben, wählen Sie **Genehmigungsaufgabe auf Eskalationsebene *<Zahl eskalieren>***. Andernfalls ist die Eskalation nicht aktiviert.
4. Klicken Sie im Feld **Die zu konfigurierende Ebene der genehmigenden Instanz wählen** auf den Eintrag, der die nächste Eskalationsebene darstellt.

   *Beispiel: Wenn Sie Eskalationsebene 1 konfigurieren, klicken Sie auf den Listeneintrag **Eskalationsebene 2**.*

5. Geben Sie genehmigende Instanzen für die folgende Eskalationsebene an (Anweisungen hierzu finden Sie unter Konfigurieren der genehmigenden Instanzen weiter vorne in diesem Dokument).

Jede Ebene der genehmigenden Instanzen besitzt eine eigene Konfiguration; damit gelten die Eskalationsoptionen einer bestimmten Ebene nur für diese Ebene. Daher gilt für jede Ebene der genehmigenden Instanzen eine eigene Frist, eine eigene Option, mit der festgelegt wird, ob die Genehmigungsaufgabe nach Ablauf der Frist eskaliert wird, und eine eigene Option, mit der festgelegt wird, ob die genehmigenden Instanzen dieser Ebene die Genehmigungsaufgabe manuell eskalieren dürfen.

Konfiguration der Anfrage nach weiteren Informationen

Sie können die Genehmigungsaktivität so konfigurieren, das die genehmigende Instanz aufgefordert wird, im Rahmen der Genehmigungsaufgabe bestimmte Eigenschaften des Objekts zu liefern. Angenommen, die Erstellung eines Benutzers wird zur Genehmigung gesendet. Die genehmigende Instanz kann aufgefordert werden, neben den in der Erstellungsanforderung genannten Eigenschaften bestimmte Eigenschaften des Benutzers anzugeben. Damit können Sie die Genehmigungsaktivität so konfigurieren, dass die genehmigende Instanz aufgefordert wird, die Postfachdatenbank für das Postfach des zu erstellenden Benutzers anzugeben.

Zum Konfigurieren der Anfrage nach weiteren Informationen gehen Sie wie folgt vor:

1. Gehen Sie zur Registerkarte **Informationsanfrage** im Dialogfeld **Eigenschaften** für die Genehmigungsaktivität.
2. Geben Sie in der Liste **Die genehmigende Instanz auffordern, diese Eigenschaften anzugeben**.

Bei der Ausführung der Genehmigungsaufgabe wird die genehmigende Instanz aufgefordert, die in dieser Liste angezeigten Eigenschaften anzugeben oder zu ändern. Die genehmigende Instanz kann die angeforderten Informationen im Abschnitt „Genehmigung" der Web-Schnittstelle unter der Überschrift **Folgende Eigenschaften angeben oder ändern** auf der Registerkarte **Objekteigenschaften** auf der Seite **Genehmigungsaufgabe** angeben. Diese Registerkarte enthält außerdem eine von der Genehmigungsaktivität angegebene Anweisung. Sie können die Anweisung auf der Registerkarte **Informationsanfrage** im Dialogfeld **Eigenschaften** für die Genehmigungsaktivität unter der Überschrift **Der genehmigenden Instanz diese Anweisung zeigen** einsehen oder ändern.

Konfiguration der Anfrage nach Prüfung

Sie können die Genehmigungsaktivität so konfigurieren, dass die genehmigende Instanz aufgefordert wird, die zur Genehmigung eingereichten Objekteigenschaften zu überprüfen. Eine weitere Option kann sein, dem Genehmiger zu gestatten, Änderungen an diesen Eigenschaften vorzunehmen.

Zum Konfigurieren der Anfrage nach Prüfung gehen Sie wie folgt vor:

1. Gehen Sie zur Registerkarte **Informationsanfrage** im Dialogfeld **Eigenschaften** für die Genehmigungsaktivität.
2. Markieren Sie das Kontrollkästchen **Der genehmigenden Instanz die ursprüngliche Anforderung zeigen**, damit die genehmigende Instanz die zur Genehmigung eingereichten Eigenschaften überprüfen kann.
3. Markieren Sie optional das Kontrollkästchen **Zulassen, dass die genehmigende Instanz die ursprüngliche Anforderung ändert**, damit die genehmigende Instanz die zur Genehmigung eingereichten Eigenschaften ändern kann.

Wenn das Kontrollkästchen **Der genehmigenden Instanz die ursprüngliche Anforderung zeigen** markiert ist, werden auf der Registerkarte **Objekteigenschaften** der Seite **Genehmigungsaufgabe** im Abschnitt „Genehmigung" des Web-Interface die zur Genehmigung eingereichten Objekteigenschaften angezeigt. Die Eigenschaftswerte werden schreibgeschützt im Bereich unter der Überschrift **Die zur Genehmigung eingereichten Eigenschaften überprüfen** angezeigt. Sie können die Genehmigungsaktivität so konfigurieren, dass die genehmigende Instanz diese Eigenschaftswerte ändern kann, indem Sie das Kontrollkästchen **Zulassen, dass die genehmigende Instanz die ursprüngliche Anforderung ändert** markieren. Wenn die genehmigende Instanz die zur Genehmigung eingereichten Eigenschaften nicht sehen können soll, löschen Sie die Markierung des Kontrollkästchens **Der genehmigenden Instanz die ursprüngliche Anforderung zeigen**.

Anpassen des Kopfes der Genehmigungsaufgaben-Seite

Sie können die Genehmigungsaktivität so konfigurieren, dass angegeben wird, wie die von dieser Aktivität erstellten Genehmigungsaufgaben im Abschnitt „Genehmigung" des Web-Interface identifiziert werden sollen. Der Abschnitt „Genehmigung" enthält eine Liste der Genehmigungsaufgaben, wobei jede Aufgabe durch eine Kopfzeile identifiziert ist, die Basisinformationen über die Aufgabe einschließlich des Titels der Aufgabe und Informationen über das Zielobjekt des zur Genehmigung eingereichten Vorgangs enthält. Der Titel der Aufgabe ist in der Mitte der Kopfzeile der Aufgabe aufgeführt. Die Eigenschaften, die das Zielobjekt des Vorgangs angeben, werden über dem Titel der Aufgabe angezeigt.

Der Titel der Genehmigungsaufgabe wird wie folgt geändert:

1. Gehen Sie zur Registerkarte **Anpassung** im Dialogfeld **Eigenschaften** für die Genehmigungsaktivität.
2. Klicken Sie auf **Den Aufgabenkopf anpassen**.
3. Geben Sie im Feld **Diese Bezeichnung zeigen, um die Genehmigungsaufgabe zu erkennen** den gewünschten Titel ein.

   *Standardmäßig lautet dieser **Vorgang genehmigen**.*

Zum Ändern der Eigenschaften, mit denen das Vorgangszielobjekt identifiziert wird, gehen Sie wie folgt vor:

1. Überprüfen Sie unter **Den Aufgabenkopf anpassen**, ob das Kontrollkästchen **Diese Eigenschaften des zur Genehmigung eingereichten Objekts anzeigen** markiert ist.
2. Verwenden Sie die Schaltflächen **Hinzufügen** und **Entfernen**, um die Liste der Eigenschaften zu konfigurieren.

   *Standardmäßig enthält die Liste die Eigenschaft **Anzeigename**; hierdurch wird ActiveRoles veranlasst, den Anzeigenamen des Objekts zu verwenden. Besitzt das Objekt keinen Anzeigenamen, verwendete ActiveRoles den Namen des Objekts.*

Standardmäßig liefert der Kopf der Genehmigungsaufgabe eine Informationsübersicht über die genehmigungspflichtigen Änderungen einschließlich der Änderungen und ihrer Begründung. Sie können den Kopf so konfigurieren, dass diese Informationen nicht angezeigt werden, indem Sie die Markierung des Kontrollkästchens **Die Vorgangsübersicht im Aufgabenkopf anzeigen** löschen.

Änderungen an der Konfiguration des Aufgabenkopfs wirken sich auf die durch die Genehmigungsaufgabe nach der Änderung erstellten Aufgaben aus, nicht auf die zuvor erstellten.

Anpassung der Aktionsschaltflächen für Genehmigung

Sie können die Genehmigungsaktivität so konfigurieren, dass die Aktionen angegeben werden, die die genehmigende Instanz an der Genehmigungsaufgabe ausführen kann. Auf den Seiten zur Durchführung der Genehmigungsaufgabe im Abschnitt „Genehmigung" des Web-Interface enthält die Kopfzeile der Aufgabe die Aktionsschaltflächen, die zur Anwendung der entsprechenden Lösung auf die Aufgabe vorgehen sind (z. B. **Genehmigen** oder **Ablehnen**). Die Aktionsschaltflächen werden unten in der Kopfzeile angezeigt. Welche Schaltflächen angezeigt werden, ist von der Konfiguration der Genehmigungsaktivität abhängig.

Zum Umbenennen oder Ausblenden von Aktionsschaltflächen gehen Sie wie folgt vor:

1. Gehen Sie zur Registerkarte **Anpassung** im Dialogfeld **Eigenschaften** für die Genehmigungsaktivität.
2. Klicken Sie auf **Aktionsschaltfläche konfigurieren**.
3. Klicken Sie auf den Titel einer Schaltfläche in der Liste und klicken Sie dann auf **Bearbeiten**.

4. Im Dialogfeld **Eigenschaften der Aktionsschaltflächen** haben Sie folgende Möglichkeiten:
   - Zum Umbenennen der Schaltfläche geben Sie den gewünschten Namen in das Feld **Beschriftung der Schaltfläche** ein.
     Der neue Namen erscheint auf der Aktionsschaltfläche im Web-Interface.
   - Zum Ausblenden der Schaltfläche löschen Sie die Markierung des Kontrollkästchens **Ist auf den Seiten für die Ausführung der Genehmigungsaufgabe sichtbar**.
     Danach wird die Aktionsschaltfläche nicht mehr im Web-Interface angezeigt.

Sie können die Aktionsschaltfläche wieder im Web-Interface anzeigen lassen, indem Sie das Kontrollkästchen **Ist auf den Seiten für die Ausführung der Genehmigungsaufgabe sichtbar** erneut markieren. Diese Option ist für die Aktionstypen „Eskalieren" und „Delegieren" nicht verfügbar. Die Schaltflächen „Eskalieren" und „Delegieren" werden im Web-Interface angezeigt, wenn die Genehmigungsaktivität der genehmigenden Instanz erlaubt, die Genehmigungsaufgabe zu eskalieren bzw. neu zuzuweisen (zu delegieren).

Die Aktionsschaltflächen sind auf den Seiten für die Ausführung der Genehmigungsaufgabe aufgeführt. Jede Schaltfläche ordnet der Aufgabe eine bestimmte Aktion zu. Es können Schaltflächen für die Erstellung benutzerdefinierter Aktionen hinzugefügt werden. Durch Klicken auf eine benutzerdefinierte Schaltfläche kann der genehmigungspflichtige Vorgang genehmigt (Aktionstyp **Abschließen**) oder zurückgewiesen werden (Aktionstyp **Ablehnen**). Wenn-Dann-Aktivitäten können je nach Titel auf eine benutzerdefinierte Aktionsschaltfläche verweisen und den geeigneten Teil des Arbeitsablaufs wählen, wenn die genehmigende Instanz diese Schaltfläche anklickt.

Zum Hinzufügen einer benutzerdefinierten Aktionsschaltfläche gehen Sie wie folgt vor:

1. Gehen Sie zur Registerkarte **Anpassung** im Dialogfeld **Eigenschaften** für die Genehmigungsaktivität.
2. Klicken Sie auf **Aktionsschaltfläche konfigurieren**.
3. Klicken Sie auf **Hinzufügen**.
4. Im Dialogfeld **Eigenschaften der Aktionsschaltflächen** gehen Sie wie folgt vor:
   a) Geben Sie im Feld **Bezeichnung der Schaltfläche** den gewünschten Namen für die Schaltfläche ein.
      Dieser Namen erscheint auf der Aktionsschaltfläche im Web-Interface.
   b) Wählen Sie aus der Liste **Aktionstyp** den gewünschten Aktionstyp für die Schaltfläche aus.
      *Bei einer Genehmigungsaufgabe bewirkt die Schaltfläche mit dem Aktionstyp **Abschließen**, dass der Arbeitsablauf fortgesetzt und die genehmigungspflichtige Aufgabe zugelassen wird; mit der Schaltfläche mit dem Aktionstyp **Ablehnen** wird der Vorgang abgelehnt.*
   c) Markieren Sie das Kontrollkästchen **Ist auf den Seiten für die Ausführung der Genehmigungsaufgabe sichtbar**.

Beim Hinzufügen benutzerdefinierter Aktionsschaltfläche empfiehlt es sich, Hinweise zur Bedeutung und zum Zweck der benutzerdefinierten Aktion zu geben. Sie können diesen Hinweistext im Feld **Diese Anweisung für die Aktionsschaltfläche zeigen** im Bereich **Aktionsschaltfläche konfigurieren** auf der Registerkarte **Anpassen** im Dialogfeld **Eigenschaften** für die Genehmigungsaktivität eingeben. Die genehmigende Instanz sieht diesen Text über den Aktionsschaltflächen auf den Seiten, auf welchen die Genehmigungsaufgabe im Web-Interface ausgeführt wird.

Um eine Genehmigungsaufgabe auszuführen, muss die genehmigende Instanz normalerweise eine Bestätigungs-Dialogbox ausfüllen. Sie können die Genehmigungsaufgabe so konfigurieren, dass das Bestätigungs-Dialogfeld nicht angezeigt wird. Markieren Sie das Kontrollkästchen **Den Bestätigungsdialog bei Abschluss der Genehmigungsaufgabe löschen** im Bereich **Aktionsschaltfläche konfigurieren** auf der Registerkarte **Anpassung** im Dialogfeld **Eigenschaften** für die Genehmigungsaktivität.

Konfigurieren einer Benachrichtigungsaktivität

Bei der Konfiguration einer Benachrichtigungsaktivität können Sie Benachrichtigungseinstellungen wie etwa Arbeitsablaufereignisse, bei deren Eintreten eine Benachrichtigung erfolgen soll, Benachrichtigungsempfänger und die Benachrichtigungsmeldungsvorlage festlegen. Diese Einstellungen gelten auch für den Benachrichtigungsabschnitt anderer Aktivitäten wie beispielsweise Genehmigungs-, Such und CRUD-Aktivitäten.

Gehen Sie folgendermaßen vor, um die Benachrichtigungseinstellungen anzuzeigen oder zu ändern:

1. Erweitern Sie in der Konsolenstruktur von ActiveRoles **Konfiguration | Richtlinien | Arbeitsablauf** und wählen Sie dann den Arbeitsablauf, der die Aktivität enthält, die Sie konfigurieren möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.
2. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Aktivität und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf die Registerkarte **Benachrichtigung** im Dialogfeld **Eigenschaften**.

Die Seite zur Konfiguration von Benachrichtigungen umfasst drei Bereiche:

- Ereignisse, Empfänger und Nachrichten In diesem Bereich können Sie Benachrichtigungen, von denen jede ein Ereignis angibt, bei dessen Eintreten eine Benachrichtigung erfolgen soll, sowie die Empfänger der Benachrichtigungsmeldung, die Nachrichtenübermittlungsoptionen und die Nachrichtenvorlage hinzufügen, anzeigen, ändern oder entfernen.
- Quest One ActiveRoles Web-Interface Dieser Bereich wird verwendet, um die Adresse (URL) des Web-Interface von Quest One ActiveRoles für die Erstellung von Hyperlinks in den Benachrichtigungsmeldungen anzugeben.
- Einstellungen des E-Mail-Servers In diesem Bereich können Sie den Namen und andere Einstellungen des E-Mail-Servers, der für die Übermittlung von Benachrichtigungsmeldungen verwendet wird, anzeigen oder ändern.

Ereignisse, Empfänger und Nachrichten

Gehen Sie folgendermaßen vor, um eine Benachrichtigung hinzuzufügen:

1. Klicken Sie im Bereich **Ereignisse, Empfänger und Nachrichten** auf **Hinzufügen**.
2. Klicken Sie im Dialogfeld **Benachrichtigungseinstellungen** unter **Ereignis auswählen** auf das Ereignis, bei dessen Eintreten eine Benachrichtigung erfolgen soll.
3. Aktivieren Sie unter **Benachrichtigungsempfänger** die entsprechenden Kontrollkästchen, um die Benachrichtigungsempfänger anzugeben.

*Die E-Mail-Adressen der auf der Seite **Benachrichtigungsempfänger** ausgewählten Empfänger wird im Feld **An** der Benachrichtigung über E-Mail-Nachrichten angezeigt. Um Empfängeradressen zum Feld **Cc** oder **Bcc** hinzuzufügen, klicken Sie auf die Schaltfläche **Kopieempfänger** bzw. **Blindkopie-Empfänger**. Hierdurch wird eine Seite geöffnet, die identisch mit der Seite **Benachrichtigungsempfänger** ist und Ihnen die Anzeige oder Änderung der Einstellung ermöglicht, welche Empfängeradressen im Feld **Cc** oder **Bcc** angezeigt werden.*

4. Wählen Sie unter **Benachrichtigungsübermittlung** die gewünschten Übermittlungsoptionen aus:
   - Wählen Sie **Sofort**, wenn die Benachrichtigungsmeldung bei jedem Eintreten des Ereignisses sofort gesendet werden soll.
   - Wählen Sie **Geplant**, wenn die Benachrichtigungsmeldungen innerhalb eines bestimmten Zeitraums gruppiert und als eine einzige Nachricht gesendet werden soll; danach geben Sie den Zeitraum an.

   *Die Option **Geplant** ist nur für das Ereignis **Aufgabe erstellt** in einer Genehmigungsaktivität verfügbar.*
5. Klicken Sie unter **Benachrichtigungsmeldung** auf **Ändern**, um die Nachrichtenvorlage einschließlich des Betreffs und des Texts der Benachrichtigungsmeldung anzuzeigen oder zu ändern.
6. Markieren Sie auf der Seite **Benachrichtigungsmeldung** das Kontrollkästchen **Einen Bericht über die Ausführung des Arbeitsablaufs als Anlage zur Benachrichtigungsmeldung beifügen**, wenn die Benachrichtigung einen Änderungsverlaufsbericht (bei einer Änderung) oder einen Ausführungsverlaufsbericht (bei einer Automatisierung) enthalten soll.

   Diese Option ist für Genehmigungsaktivitäten nicht verfügbar.
7. Klicken Sie auf **OK**, um das Dialogfeld **Benachrichtigungseinstellungen** zu schließen.

Für das Ereignis **Aufgabe erstellt** in einer Genehmigungsaktivität kann die Benachrichtigung so konfiguriert werden, dass Benachrichtigungsmeldungen in Gruppen zusammengefasst und nach einem Zeitplan versandt werden. Wenn Sie die Option **Geplant** unter **Benachrichtigungsübermittlung** auswählen, werden die Nachrichten innerhalb eines bestimmten, geplanten Zeitraums in einem temporären Speicher gesammelt, anstatt bei Eintritt des Ereignisses sofort gesendet zu werden. Nach Ablauf der festgelegten Dauer werden alle zusammengefassten Nachrichten als eine einzige Nachricht gesendet. Sie können die Aktivität so konfigurieren, dass Benachrichtigungen täglich oder stündlich übermittelt werden.

Durch Klicken auf die Schaltfläche **Ändern** unter **Benachrichtigungsmeldung** wird ein Fenster geöffnet, in dem Sie die E-Mail-Benachrichtigungsvorlagen anzeigen und ändern können. Die Benachrichtigungskonfiguration definiert für jeden Ereignistyp eine Standardvorlage; auf der Basis dieser Vorlage verfasst Quest One ActiveRoles E-Mail-Benachrichtigungsmitteilungen. Jede Vorlage umfasst ein XHTML-Markup sowie den Text und Token, die Informationen über das Ereignis enthalten.

Damit die Benachrichtigungsmeldungen für die Empfänger aussagekräftiger sind, bieten Benachrichtigungsvorlagen die Möglichkeit, Token in die Nachrichten aufzunehmen, die zusätzliche Informationen über das Ereignis enthalten. Klicken Sie auf die Schaltfläche **Token einfügen**, um eine Liste der verfügbaren Token anzuzeigen. Die Liste enthält eine Kurzbeschreibung für jeden Token.

Sie können Vorlagen bearbeiten, um den Inhalt und das Format von Benachrichtigungs-E-Mails anzupassen. Die Änderungen an den Vorlagen sind benachrichtigungsspezifisch und ereignisspezifisch: Wenn Sie die Vorlage für ein bestimmtes Ereignis innerhalb der Konfiguration einer bestimmten Benachrichtigung ändern, haben Ihre Änderungen keine Auswirkungen auf andere Benachrichtigung oder Ereignisse. Dies ermöglicht, dass unterschiedliche Benachrichtigungen und Ereignisse über verschiedene, benutzerdefinierte Benachrichtigungsvorlagen verfügen.

Gehen Sie folgendermaßen vor, um eine Benachrichtigung anzuzeigen oder zu ändern:

1. Wählen Sie einen Eintrag aus der Liste im Bereich **Ereignisse, Empfänger und Nachrichten** und klicken Sie dann auf **Bearbeiten**.
2. Verwenden Sie das Dialogfeld **Benachrichtigungseinstellungen** wie weiter oben in diesem Abschnitt beschrieben.

Gehen Sie folgendermaßen vor, um eine Benachrichtigung zu löschen:

- Wählen Sie den entsprechenden Eintrag aus der Liste im Bereich **Ereignisse, Empfänger und Nachrichten** und klicken Sie dann auf **Entfernen**.

Quest One ActiveRoles Web-Interface

Die in diesem Bereich angegebene Adresse (URL) wird verwendet, um Hyperlinks in den Benachrichtigungsmeldungen zu erstellen, sodass die Benachrichtigungsempfänger leicht auf Web-Interface-Seiten für die Durchführung von Arbeitsablaufaufgaben zugreifen können.

Gehen Sie folgendermaßen vor, um die Adresse des Web-Interface von Quest One ActiveRoles anzugeben:

1. Geben Sie im Bearbeitungsfeld unter **Quest One ActiveRoles Web-Interface** die Adresse (URL) der Quest One ActiveRoles Web-Interface-Seite ein (beispielsweise http://<server>/ARServerAdmin).
2. Klicken Sie auf **Test**, um die Adresse zu überprüfen. Wenn die Adresse richtig ist, öffnet sich die Web-Interface-Seite in Ihrem Webbrowser.

Einstellungen des E-Mail-Servers

Die in diesem Bereich angegebenen Einstellungen legen den für die Benachrichtigungsübermittlung zu verwendenden Server fest.

Gehen Sie folgendermaßen vor, um die E-Mail-Servereinstellungen zu konfigurieren:

1. Klicken Sie im Bereich **E-Mail-Server-Einstellungen** auf **Eigenschaften**.
2. Verwenden Sie das Dialogfeld **Eigenschaften**, um die E-Mail-Servereinstellungen anzuzeigen oder zu ändern.

Gehen Sie folgendermaßen vor, um eine andere E-Mail-Serverkonfiguration auszuwählen:

- Klicken Sie auf den Namen der gewünschten Konfiguration in der Liste **Konfiguration des Servers für ausgehende Nachrichten**.

Gehen Sie folgendermaßen vor, um eine E-Mail-Serverkonfiguration zu erstellen:

- Erweitern Sie in der Konsolenstruktur von Quest One ActiveRoles **Konfiguration | Server-Konfiguration**, klicken Sie mit der rechten Maustaste auf **Mail-Konfiguration** und wählen Sie **Neu | Mail-Konfiguration**.

Konfigurieren einer Skriptaktivität

Bei der Konfiguration einer Skriptaktivität wählen Sie das Skriptmodul aus, das das Skript enthält, das von der Aktivität verwendet werden soll. Anschließend wählen Sie unter den im Skript enthaltenen Funktionen die Funktion, die von der Aktivität ausgeführt werden soll, und optional die Funktion, die die Aktivitätsparameter deklariert, aus. Wenn irgendwelche Parameter deklariert sind, müssen Sie Parameterwerte für diese Parameter angeben. Informationen und Anweisungen bezüglich der Erstellung eines Skripts für eine Skriptaktivität finden Sie im Quest One ActiveRoles SDK.

Gehen Sie folgendermaßen vor, um eine Skriptaktivität zu konfigurieren:

1. Erweitern Sie in der Quest One ActiveRoles Konsolenstruktur **Configuration | Policies | Workflow** und wählen Sie dann den Arbeitsablauf, der die Skriptaktivität enthält, die Sie konfigurieren möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.

2. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Aktivität und klicken Sie dann auf **Eigenschaften**.
3. Gehen Sie zur Registerkarte **Allgemein** im Dialogfeld **Eigenschaften der Skriptaktivität**.
4. Führen Sie einen der nachfolgend aufgeführten Schritte aus:
   - Wenn für die Aktivität kein Skriptmodul ausgewählt ist (beispielsweise wenn die Aktivität gerade zum Prozessdiagramm hinzugefügt wurde), klicken Sie auf **Durchsuchen** und wählen dann das Skriptmodul aus, das das Skript enthält, das die Aktivität verwenden soll.
   - Wenn für die Aktivität bereits ein Skriptmodul ausgewählt ist und Sie ein anderes Skriptmodul verwenden möchten, klicken Sie auf die Schaltfläche **Durchsuchen**, um das gewünschte Skriptmodul auszuwählen.
5. Im Feld **Auszuführende Funktion** wird der Name der Skriptfunktion angezeigt, die von dieser Aktivität ausgeführt wird. Sie können die gewünschte Funktion aus der Liste **Auszuführende Funktion** auswählen.

   *Die Liste enthält die Namen aller im ausgewählten Skriptmodul gefundenen Skriptfunktionen. Die Aktivität führt die im Feld **Auszuführende Funktion** angegebene Funktion aus.*

6. Im Feld **Funktion zur Deklaration von Parametern** wird der Name der Funktion angezeigt, die die Aktivitätsparameter definiert. Klicken Sie auf **Parameter festlegen** und gehen Sie dann wie folgt vor:
   a) Wählen Sie erforderlichenfalls aus der Liste **Funktion zur Deklaration von Parametern** die Funktion aus, die die für diese Aktivität spezifischen Parameter definiert.

      *Die Liste enthält die Namen aller im ausgewählten Skriptmodul gefundenen Skriptfunktionen. Die Aktivität verfügt über die Parameter, die von der Funktion definiert sind, die im Feld **Funktion zur Deklaration von Parametern** angegeben ist. Normalerweise ist dies eine Funktion mit der Bezeichnung „onInit".*

   b) Zeigen Sie unter **Parameterwerte** die Werte der Aktivitätsparameter an oder ändern Sie sie. Um den Wert eines Parameters zu ändern, wählen Sie den Namen des Parameters aus und klicken Sie dann auf **Bearbeiten**.

      *Durch Anklicken von **Bearbeiten** wird eine Seite angezeigt, auf der Sie einen oder mehrere Werte für den ausgewählten Parameter hinzufügen, entfernen oder auswählen können. Für jeden Parameter definiert die Funktion, die für die Deklaration von Parametern verwendet wird, den Namen des Parameters und andere Merkmale wie etwa eine Beschreibung, eine Liste der möglichen Werte, den Standardwert und ob ein Wert erforderlich ist oder nicht. Wenn eine Liste der möglichen Werte definiert ist, dann können Sie nur Werte aus dieser Liste auswählen.*

7. Optional gehen Sie zur Registerkarte **Benachrichtigung** im Dialogfeld **Eigenschaften der Skriptaktivität** und abonnieren Sie anhand der Schritte für Konfigurieren einer Benachrichtigungsaktivität Empfänger für die Benachrichtigung bei folgenden Ereignissen:
   - **Aktivität erfolgreich abgeschlossen.** Wenn diese Aktivität so konfiguriert wurde, dass Benachrichtigungen über dieses Ereignis erfolgen, versendet ActiveRoles eine Benachrichtigungs-E-Mail, wenn während der Ausführung dieser Aktivität keine erheblichen Fehler festgestellt wurden.
   - **Aktivität hat einen Fehler festgestellt.** Wenn diese Aktivität so konfiguriert wurde, dass Benachrichtigungen über dieses Ereignis erfolgen, versendet ActiveRoles eine Benachrichtigungs-E-Mail, wenn während der Ausführung dieser Aktivität erhebliche Fehler festgestellt wurden.
8. Optional gehen Sie zur Registerkarte **Fehlerbehebung** im Dialogfeld **Eigenschaften der Skriptaktivität** und markieren bzw. löschen Sie die Markierung des Kontrollkästchens **Arbeitsablauf fortsetzen, auch wenn bei dieser Aktivität ein Fehler festgestellt wird**, um festzulegen, ob ActiveRoles Fehlermeldungen bei dieser Skriptaktivität unterdrücken soll.

   Ist dieses Kontrollkästchen nicht markiert (Standardeinstellung), führt ein bei der Aktivität festgestellter Fehler dazu, dass ActiveRoles den Arbeitsablauf beendet. Wenn Sie dieses Kontrollkästchen markieren, wird der Arbeitsablauf unabhängig davon, ob bei der Aktivität ein Fehler erkannt wird, fortgesetzt.

Konfigurieren einer Wenn-Dann-Sonst-Aktivität

Eine Wenn-Dann-Sonst-Aktivität ist eine zusammengesetzte Aktivität. Sie besteht aus mehreren Zweigen. Für jeden dieser Zweige sind individuelle Bedingungen angegeben. Ein Wenn-Dann-Sonst-Zweig kann eine beliebige Anzahl anderer Aktivitäten enthalten. Jeder Vorgang, der die für einen bestimmten Zweig angegebenen Bedingungen erfüllt, führt dazu, dass ActiveRoles die in diesem Zweig enthaltenen Aktivitäten ausführt. Es kann nur ein Zweig einer einzelnen Wenn-Dann-Sonst-Aktivität ausgeführt werden, selbst wenn der Vorgang die Bedingungen von mehr als einem Zweig erfüllt.

Normalerweise hat eine Wenn-Dann-Sonst-Aktivität zwei Zweige, wobei für den ersten (äußersten linken) Zweig bestimmte Bedingungen angegeben sind. Für den zweiten Zweig sind keine Bedingungen angegeben, sodass er als der „Sonst"-Zweig fungiert. Wenn ein Vorgang die Bedingungen erfüllt, werden die im ersten Zweig enthaltenen Aktivitäten ausgeführt; andernfalls führt der Vorgang die im zweiten Zweig gefundenen Aktivitäten aus.

Die Konfiguration einer Wenn-Dann-Sonst-Aktivität umfasst die folgenden Aufgaben:

- Hinzufügen eines Zweigs
- Hinzufügen von Aktivitäten zu einem Zweig
- Konfiguration von Zweigbedingungen (siehe Konfigurieren von Bedingungen für einen Wenn-Dann-Zweig)
- Konfiguration der Fehlerbehebung (siehe Schritte zur Konfiguration der Fehlerbehebung)

Gehen Sie folgendermaßen vor, um einen Zweig zu einer Wenn-Dann-Sonst-Aktivität hinzuzufügen:

1. Erweitern Sie in der Konsolenstruktur von Quest One ActiveRoles **Configuration | Policies | Workflow** und wählen Sie dann den Arbeitsablauf, der die Wenn-Dann-Aktivität enthält, die Sie konfigurieren möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.

2. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Wenn-Dann-Sonst-Aktivität und klicken Sie dann auf **Zweig hinzufügen**.

Hierdurch wird ein Zweig mit dem Standardnamen „Wenn-Dann-Sonst-Zweig" hinzugefügt. Klicken Sie mit der rechten Maustaste auf den Namen des Zweigs und klicken Sie dann auf **Eigenschaften**, um den Namen wie gewünscht zu ändern. Sie können einen Zweig löschen, indem Sie auf seinen Name und dann auf **Löschen** klicken.

Gehen Sie folgendermaßen vor, um eine Aktivität zu einem Wenn-Dann-Sonst-Zweig hinzuzufügen:

- Ziehen Sie die Aktivität vom linken Bereich auf den Zweig.

Wenn Sie eine Aktivität zum oberen Teil des Diagramms hinzufügen (über der Zeile **Vorgangsausführung**), dann wird die Aktivität in der Vorausführungsphase der Vorgangsverarbeitung ausgeführt (siehe „Übersicht über den Arbeitsablaufprozess" weiter oben in diesem Kapitel).

Wenn Sie eine Aktivität zum unteren Teil des Diagramms hinzufügen (unter der Zeile **Vorgangsausführung**), dann wird die Aktivität in der Nachausführungsphase der Vorgangsverarbeitung ausgeführt. Bestimmte Aktivitäten wie etwa eine Genehmigungsaktivität, die für eine Aufführung in der Vorausführungsphase konzipiert sind, können nicht zum unteren Teil des Diagramms hinzugefügt werden.

Sie können eine Aktivität von einem Zweig löschen, indem Sie den Namen der Aktivität und dann auf **Löschen** klicken.

Das folgende Thema enthält Anweisungen für die Konfiguration von Bedingungen für einen Wenn-Dann-Zweig: Konfigurieren von Bedingungen für einen Wenn-Dann-Zweig.

Schritte zur Konfiguration der Fehlerbehebung

Bei der Konfiguration einer Wenn-Dann-Aktivität können Sie die Fehlerbehebung so konfigurieren, dass Fehler, die bei dieser Wenn-Dann-Aktivität und allen in dieser Aktivität enthaltenen Aktivitäten festgestellt werden, unterdrückt werden.

Gehen Sie zum Konfigurieren der Fehlerbehebung für eine Wenn-Dann-Aktivität wie folgt vor:

1. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Wenn-Dann-Aktivität und klicken Sie dann auf **Eigenschaften**.
2. Gehen Sie zur Registerkarte **Fehlerbehebung** im Dialogfeld **Eigenschaften der Wenn-Dann-Genehmigungsaktivität** und markieren Sie das Kontrollkästchen **Arbeitsablauf fortsetzen, auch wenn bei dieser Aktivität ein Fehler festgestellt wird** auf dieser Registerkarte bzw. löschen Sie die Markierung.

Wenn **Arbeitsablauf fortsetzen, auch wenn bei dieser Aktivität ein Fehler festgestellt wird** markiert ist (Standardeinstellung), beendet ActiveRoles bei einem bei dieser Aktivität festgestellten Fehler den Arbeitsablauf. Wenn Sie dieses Kontrollkästchen markieren, wird der Arbeitsablauf unabhängig davon fortgesetzt, ob bei der Wenn-Dann-Aktivität oder einer darin enthaltenen Aktivität ein Fehler festgestellt wird.

Konfigurieren von Bedingungen für einen Wenn-Dann-Zweig

Eine Wenn-Dann-Aktivität ist darauf ausgelegt, genau einen Zweig der Aktivität aus einer Reihe von Zweigen auszuwählen. Bei jedem Zweig überprüft die Aktivität die Zweigbedingungen und führt den ersten jener Zweige aus, dessen Bedingung zu WAHR ausgewertet wird.

Der Workflow Designer enthält einen Condition Builder für die Konfiguration von Zweigbedingungen; dieser wird über das Dialogfeld **Aktivitätseigenschaften des Wenn-Dann-Zweigs** aufgerufen.

Der Condition Builder für einen Wenn-Dann-Zweig wird wie folgt aufgerufen:

1. Klicken Sie mit der rechten Maustaste auf den Namen des Zweigs und klicken Sie dann auf **Eigenschaften**.
2. Gehen Sie im daraufhin geöffneten Dialogfeld **Aktivitätseigenschaften des Wenn-Dann-Zweigs** zum Feld **Eigenschaften**.

Bei der Konfiguration eines Wenn-Dann-Zweigs müssen Sie mindestens eine Bedingung hinzufügen. Standardmäßig wird eine einzelne, implizite Bedingungsgruppe erstellt, wenn Sie eine Zweigbedingung hinzufügen. Sie können weitere Bedingungsgruppen erstellen, um eine Reihe von Bedingungen zu gruppieren und um gruppierte Bedingungen innerhalb anderer Bedingungsgruppen zu verschachteln.

Eine Bedingungsgruppe enthält eine oder mehrere Bedingungen, die durch denselben logischen Operator miteinander verbunden sind. Durch die Gruppierung von Bedingungen geben Sie an, dass diese Bedingungen als eine Einheit bewertet werden sollen. Der Effekt ist derselbe, als wenn Sie einen Ausdruck in einer mathematischen Gleichung oder in einer logischen Aussage in Klammern setzen.

Um eine Bedingung in einer Bedingungsgruppe hinzuzufügen

- Klicken Sie im Feld **Bedingungen** auf den Namen der Bedingungsgruppe und danach auf **Bedingung hinzufügen**.

  – ODER –

  Klicken Sie auf das Pluszeichen (+) neben dem Namen der Bedingungsgruppe.

Bei Bedarf können Sie eine Bedingung entfernen, indem Sie auf die mit einem **X** gekennzeichnete Schaltfläche **Bedingung löschen** rechts neben dem Listeneintrag für die Bedingung im Feld **Bedingungen** klicken.

Eine Bedingungsgruppe in einer anderen Bedingungsgruppe hinzufügen

- Klicken Sie im Feld **Bedingungen** auf denn Namen der Bedingungsgruppe, zeigen Sie auf **Bedingungsgruppe einfügen** und klicken Sie zur Angabe des logischen Operators auf die entsprechende Option:
  - **AND-Gruppe.** Die Bedingungsgruppe wertet zu TRUE aus, wenn alle Bedingungen in der Gruppe TRUE sind.
  - **OR-Gruppe.** Die Bedingungsgruppe wertet zu TRUE aus, wenn jede Bedingung in der Gruppe TRUE ist.
  - **NOT AND-Gruppe.** Die Bedingungsgruppe wertet zu TRUE aus, wenn jede Bedingung zu FALSE wertet.
  - **NOT AND-Gruppe.** Die Bedingungsgruppe wertet zu TRUE aus, wenn jede Bedingung zu FALSE wertet.

Standardmäßig ist AND der logische Operator zwischen den Bedingungen in einer Bedingungsgruppe. Es ist möglich, die logische Verknüpfung durch Konvertieren der Bedingungsgruppe in einen anderen Gruppentyp zu ändern. Klicken Sie auf den Namen der Gruppe, gehen Sie auf **Bedingungsgruppe konvertieren** und klicken Sie auf die der gewünschten logischen Verknüpfung entsprechende Option.

Sie können auch eine gesamte Bedingungsgruppe entfernen, indem Sie auf den Namen der Gruppe und dann auf **Bedingungsgruppe löschen** klicken.

Wenn Sie eine Bedingung in einer Bedingungsgruppe hinzugefügt haben, können Sie mit den folgenden Schritten die Bedingungen konfigurieren.

Eine Bedingung konfigurieren

1. Klicken Sie auf **Zu bewertende Bedingung konfigurieren** und wählen Sie unter den folgenden Optionen, um die Entität oder das Feld, die nach der Bedingung bewertet werden sollen, anzugeben:
   - **Eigenschaft des Arbeitsablaufzielobjekts.** Bewertet den Wert einer bestimmten Eigenschaft des Zielobjekts der Anfrage, die den Arbeitsablauf gestartet hat. Der Condition Builder fordert Sie zur Auswahl der gewünschten Eigenschaft auf. Diese Option ist bei Automatisierungs-Arbeitsabläufen nicht verfügbar.
   - **Eigenschaft des Arbeitsablaufinitiators.** Bewertet den Wert einer bestimmten Eigenschaft des Benutzers, dessen Anfrage den Arbeitsablauf gestartet hat. Der Condition Builder fordert Sie zur Auswahl der gewünschten Eigenschaft auf.
   - **Geänderter Wert der Eigenschaft des Arbeitsablaufzielobjekts.** Bewertet den Wert, der laut Anfrage einer bestimmten Eigenschaft des Arbeitsablaufzielobjekts zugewiesen werden soll. Dieser steht für die angeforderte Änderung der Eigenschaft des Zielobjekts der Anfrage, die den Arbeitsablauf gestartet hat. Der Condition Builder fordert Sie zur Auswahl der gewünschten Eigenschaft auf. Diese Option ist bei Automatisierungs-Arbeitsabläufen nicht verfügbar.
   - **Ausführungsstatus der Aktivität.** Bewertet, ob ActiveRoles bei der Ausführung einer bestimmten Aktivität einen Fehler festgestellt hat. Der Condition Builder fordert Sie zur Auswahl der gewünschten Eigenschaft auf. Beachten Sie, dass es bei dieser Option erforderlich ist, dass die Aktivitätskonfiguration die Fortsetzung des Arbeitsablaufs auch dann gestattet, wenn die Aktivität einen Fehler feststellt.
   - **Gewählte Aktion genehmigen.** Bewertet den Namen der von der genehmigenden Instanz zum Abschluss der von einer bestimmten Genehmigungsaktivität erzeugten Genehmigungsaufgabe verwendeten Aktionsschaltfläche. Verwenden Sie diese Option, um festzulegen, welche Aktionsschaltfläche die genehmigende Instanz verwendet hat, um den genehmigungspflichtigen Vorgang zuzulassen. Der Condition Builder fordert Sie zur Auswahl der gewünschten Genehmigungseigenschaft auf. Diese Option ist bei Automatisierungs-Arbeitsabläufen nicht verfügbar.
   - **Arbeitsablaufparameterwert.** Bewertet den Wert eines bestimmten Parameters des Arbeitsablaufs. Der Condition Builder fordert Sie zur Auswahl des gewünschten Parameters aus der Arbeitsablaufdefinition auf.
   - **Eigenschaft des Objekts aus dem Arbeitsablaufdatenkontext.** Bewertet den Wert einer bestimmten Eigenschaft des Objekts, das bei Ausführung des Arbeitsablaufs auf der Basis der in der Arbeitsablaufumgebung festgestellten Daten von der Wenn-Dann-Aktivität ausgewählt wird. Der Condition Builder fordert Sie auf, die gewünschte Eigenschaft zu wählen und anzugeben, welches Objekt von der Aktivität bei Bewertung der Bedingung während der Ausführung des Arbeitsablaufs ausgewählt werden soll.
   - **Wert durch Regel-Ausdruck generiert.** Bewertet den Zeichenfolgenwert eines bestimmten Regel-Ausdrucks. Der Condition Builder fordert Sie zur Konfiguration eines Regel-Ausdrucks auf. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. ActiveRoles errechnet den Wert Ihres Regel-Ausdrucks bei der Auswertung der Bedingung zum Ausführungszeitpunkt des Arbeitsablaufs.
2. Klick Sie bei Bedarf auf den aktuellen Vergleichsoperator und dann auf den Operator, den die Bedingung verwenden soll.
3. Klicken Sie auf **Wert definieren zum Vergleich mit** und wählen Sie eine Option für die Angabe des gewünschten Vergleichswerts.

Die Liste der Optionen, die zur Angabe eines Vergleichswertes zur Verfügung stehen, hängt von der Einheit oder dem Feld ab, auf deren bzw. dessen Auswertung die Bedingung konfiguriert wurde. In der folgenden Tabelle werden die Vergleichswertoptionen zusammengefasst.

AUSZUWERTENDE BEDINGUNG	VERGLEICHSWERTOPTIONEN
Eigenschaft des Arbeitsablaufzielobjekts – ODER – Eigenschaft des Arbeitsablaufinitiators – ODER – Geänderter Wert der Eigenschaft des Arbeitsablaufzielobjekts – ODER – Arbeitsablaufparameterwert – ODER – Eigenschaft des Objekts aus dem Arbeitsablaufdatenkontext – ODER – Durch Regel-Ausdruck generierter Wert	• Textzeichenfolge • Eigenschaft des Arbeitsablaufzielobjekts • Eigenschaft des Arbeitsablaufinitiators • Geänderter Wert der Eigenschaft des Arbeitsablaufzielobjekts • Arbeitsablaufparameterwert • Eigenschaft des Objekts aus dem Arbeitsablaufdatenkontext • Durch Regel-Ausdruck generierter Wert
Ausführungsstatus der Aktivität	• Nicht ausgeführt • Erfolgreich abgeschlossen • Einen Fehler festgestellt
Gewählte Aktion genehmigen	• Der Name einer Aktionsschaltfläche • Vom Skript generierter Wert

Eine Kurzbeschreibung der Vergleichsoperatoren und Vergleichswertoptionen finden Sie unter Suchfilter.

Konfiguration einer skriptbasierten Bedingung

Um eine skriptbasierte Bedingung zu konfigurieren, müssen Sie ein Skriptmodul erstellen und anwenden, das eine Funktion enthält, die den angeforderten Vorgang analysiert, um zu ermitteln, ob der Zweig ausgeführt werden soll oder nicht. Die Funktion kann den ADSI-Provider von Quest One ActiveRoles verwenden, um auf die Eigenschaften der am Vorgang beteiligten Objekte zuzugreifen, um die Eigenschaften zu analysieren und um dann abhängig von den Ergebnissen der Analyse den Wert TRUE oder FALSE auszugeben. Der Zweig wird ausgeführt, wenn die Funktion TRUE ausgibt.

Gehen Sie folgendermaßen vor, um die skriptbasierte Bedingung anzuwenden:

1. Klicken Sie mit der rechten Maustaste auf den Namen des Zweigs und klicken Sie dann auf **Eigenschaften**.
2. Gehen Sie im Dialogfeld **Aktivitätseigenschaften des Wenn-Dann-Zweigs** unter **Bedingungen** wie folgt vor:
   a) Klicken Sie auf den Titel der Bedingungsgruppe und danach auf **Bedingung einfügen**.
   b) Klicken Sie auf **Zu bewertende Bedingung konfigurieren** und danach auf **Wert durch Regel-Ausdruck generiert**.
3. Klicken Sie im Dialogfeld **Regelausdruck konfigurieren** auf **Eingabe hinzufügen** und dann auf **Durch Skript generierter Wert**.

4. Wählen Sie im Dialogfeld **Eingabe konfigurieren** das entsprechende Skriptmodul und die entsprechende Skriptfunktion.
5. Klicken Sie auf **OK**, um das Dialogfeld **Eingabe konfigurieren** zu schließen.
6. Klicken Sie auf **OK**, um das Dialogfeld **Regelausdruck konfigurieren** zu schließen.
7. Gehen Sie im Dialogfeld **Aktivitätseigenschaften des Wenn-Dann-Zweigs** unter **Bedingungen** wie folgt vor:
   a) Überprüfen Sie, ob der Vergleichsoperator **gleich** gewählt ist.
   b) Klicken Sie auf **Wert definieren zum Vergleich mit** und danach auf **Textzeichenfolge**.
8. Geben Sie im Dialogfeld **Eingabe konfigurieren** unter **Textfolge** TRUE ein.
9. Klicken Sie auf **OK**, um das Dialogfeld **Eingabe konfigurieren** zu schließen.
10. Klicken Sie auf **OK**, um das Dialogfeld **Aktivitätseigenschaften des Wenn-Dann-Zweigs** zu schließen.
11. Speichern Sie ihre Änderungen an der Arbeitsablaufdefinition.

Dadurch wird der von Ihnen konfigurierte Wenn-Dann-Zweig ausgewählt, wenn die in Schritt 4 angegebene Funktion bei Ausführung des Arbeitsablaufs TRUE ergibt. Weitere Informationen und Anweisungen erhalten Sie unter „Entwicklung von Skriptbedingungsfunktionen" in Quest One ActiveRoles SDK.

Konfigurieren einer Stoppen/Unterbrechen-Aktivität

Bei der Konfiguration einer Stoppen/Unterbrechen-Aktivität können Sie den Text einer Informationsmeldung angeben. Die Aktivität beendet die Arbeitsablaufinstanz und meldet das entsprechende Ereignis an das „EDM-Server"-Ereignisprotokoll. Die Nachricht ist in der Ereignisbeschreibung enthalten. Wenn möglich, zeigt die Aktivität außerdem die Meldung auf der Client-Benutzeroberfläche (beispielsweise Quest One ActiveRoles Konsole oder Web-Interface) an, von der aus der Vorgang angefordert wurde der den Arbeitsablauf gestartet hat.

Gehen Sie folgendermaßen vor, um eine Stoppen/Unterbrechen-Aktivität zu konfigurieren:

1. Erweitern Sie in der Konsolenstruktur von Quest One ActiveRoles **Konfiguration | Richtlinien | Arbeitsablauf** und wählen Sie dann den Arbeitsablauf, der die Stoppen/ Unterbrechen-Aktivität enthält, die Sie konfigurieren möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.
2. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Aktivität und klicken Sie dann auf **Eigenschaften**.
3. Lassen Sie den Meldungstext im Feld **Informationsmeldung** anzeigen und ändern Sie ihn bei Bedarf.

Konfiguration einer Aktivität „Berichtsabschnitt hinzufügen"

Sie können mit einer Aktivität „Berichtsabschnitt hinzufügen" benutzerdefinierte Informationen zum Änderungsverlaufsbericht (bei einem durch eine Vorgangsanforderung gestarteten Arbeitsablauf oder zum Ausführungsverlaufsbericht (bei einem Automatisierungs-Arbeitsablauf) hinzufügen. Mit dieser Aktivität wird zum Bereich „Arbeitsablaufaktivitäten und Richtlinienaktionen" des Reports ein neuer Abschnitt hinzugefügt. Der Abschnitt besteht aus einem Kopf- und Textteil. Bei der Konfiguration einer Aktivität „Berichtsabschnitt hinzufügen" geben Sie an, welche Informationen im Kopf und im Text enthalten sein sollen.

Gehen Sie zum Konfigurieren einer Aktivität „Berichtsabschnitt hinzufügen" wie folgt vor:

1. Erweitern Sie in der Konsolenstruktur von Quest One ActiveRoles **Konfiguration | Richtlinien | Arbeitsablauf** und wählen Sie dann den Arbeitsablauf, der die Aktivität „Berichtsabschnitt hinzufügen" enthält, die Sie konfigurieren möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.

2. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Aktivität und klicken Sie dann auf **Eigenschaften**.
3. Wählen Sie unter **Dieser Berichtsabschnitt dient dazu, Informationen anzuzeigen** die Option **Einen Fehlerzustand**, wenn der Report den Text seines Kopfs und seines Texts in Rot anzeigen soll. Andernfalls wählen Sie **Einen erfolgreichen Vorgang**.
4. Klicken Sie unter **Kopf des Berichtsabschnitts** zum Verfassen des Kopftexts auf **Definieren**. Die folgenden Optionen sind verfügbar:
   - **Textzeichenfolge.** Zur Angabe einer Zeichenfolge, die als Kopf des Berichtsabschnitts angezeigt werden soll. Der Workflow Designer fordert Sie zur Eingabe der gewünschten Zeichenfolge auf.
   - **Wert durch Regel-Ausdruck generiert.** Zum Verfassen des Kopftexts von Dateneinträgen, die während der Ausführung der Aktivität berechnet werden sollen. Der Workflow Designer fordert Sie zur Konfiguration einer Reihe von Einträgen auf und bietet verschiedene Eintragstypen an, die bewirken, dass der Kopftext Eigenschaften von am Arbeitsablauf beteiligten Objekten und von damit in Zusammenhang stehenden Objekten, Datum und Uhrzeit der Aktivitätsausführung und Arbeitsablaufparameter enthalten kann.
5. Klicken Sie unter **Text des Berichtsabschnitts** auf **Text hinzufügen** und wählen Sie für die Konfiguration des Texts des Berichtsabschnitts eine der folgenden Optionen:
   - **Textzeichenfolge.** Zum Hinzufügen einer Zeichenfolge. Der Workflow Designer fordert Sie zur Eingabe der gewünschten Zeichenfolge auf.
   - **Datum und Uhrzeit des Arbeitsablaufs.** Zum Hinzufügen einer Zeichenfolge für das Datum und die Uhrzeit, zu dem bzw. der die Aktivität bei der Ausführung des Arbeitsablaufs gestartet wurde (im Workflow Designer als aktuelles Datum und aktuelle Uhrzeit bezeichnet). Sie können das Format der Zeichenfolge für Datum und Uhrzeit ändern und bei Bedarf eine Zeitverschiebung in Tagen angeben.
   - **Arbeitsablaufparameterwert.** Zum Hinzufügen einer von einem bestimmten Parameter des Arbeitsablaufs angegebenen Zeichenfolge. Der Workflow Designer fordert Sie zur Auswahl des gewünschten Parameters auf.
   - **Zeilenumbruchzeichen (CR/LF).** Zum Festlegen des Codes für Zeilenende und Beginn einer neuen Zeichenfolge.
   - **Tabulaturzeichen.** Zum Hinzufügen eines Tabulaturzeichens zur Zeichenfolge.
   - **Aufzählungszeichen.** Zum Hinzufügen eines Aufzählungszeichens zur Zeichenfolge. Sie können mit einem Punkt und einem Tabulaturzeichen am Anfang einer Zeichenfolge diese als punktgegliederten Listeneintrag formatieren.
   - **Eigenschaft des Objekts aus dem Arbeitsablaufdatenkontext.** Fügt den Wert einer bestimmten Eigenschaft des Objekts hinzu, das bei Ausführung des Arbeitsablaufs auf der Basis der in der Arbeitsablaufumgebung festgestellten Daten von der Aktivität ausgewählt wird. Der Workflow Designer fordert Sie auf, die gewünschte Eigenschaft zu wählen und anzugeben, welches Objekt von der Aktivität bei Erstellung des Berichtsabschnitts während der Ausführung des Arbeitsablaufs ausgewählt werden soll.

Im Feld **Text des Berichtsabschnitts** können Sie Texteinträge ändern, umsortieren oder löschen. Zum Ändern eines Texteintrags klicken Sie auf den Text und danach auf **Bearbeiten**. Zum Umsortieren oder Löschen von Texteinträgen verwenden Sie die Schaltflächen rechts neben den Listeneinträgen für die Texteinträge im Feld **Text des Berichtsabschnitts**. Somit klicken Sie zum Löschen eines Eintrags auf die Schaltfläche **X** rechts neben dem Listeneintrag für diesen Text im Feld **Text des Berichtsabschnitts**.

Konfigurieren einer Suchaktivität

Mit einer Suchaktivität können Sie Verzeichnisse nach Objekten wie beispielsweise Benutzern oder Gruppen durchsuchen, die den Suchkriterien entsprechen, die Sie auf der Basis von Objekteigenschaften, Objektspeicherort und anderen in der Ausführungsumgebung des Arbeitsablaufs verfügbaren Informationen angeben. Diese Objekte können Sie an andere Aktivitäten weitergeben, sodass der Arbeitsablauf die entsprechenden Aktionen mit ihnen ausführen kann. Sie können Aktivitäten in eine Suchaktivität einfügen und von diesen Aktivitäten die von der Suchaktivität gefundenen Objekte verarbeiten lassen.

Gehen Sie folgendermaßen vor, um eine Aktivität zu einer Suchaktivität hinzuzufügen:

1. Erweitern Sie in der Konsolenstruktur von Quest One ActiveRoles **Konfiguration | Richtlinien | Arbeitsablauf** und wählen Sie dann den Arbeitsablauf, der die Suchaktivität enthält.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.

2. Ziehen Sie im Bereich „Details" die Aktivität vom linken Bereich auf die Suchaktivität im Prozessdiagramm.

Zum Konfigurieren einer Suchaktivität klicken Sie mit der rechten Maustaste auf den Namen der Aktivität im Prozessdiagramm und klicken Sie dann auf **Eigenschaften**. Danach führen Sie im Dialogfeld **Eigenschaften der Suchaktivität** folgende Aufgaben aus:

- Konfiguration von Bereich und Filter
- Konfiguration einer Benachrichtigung
- Konfigurieren der Fehlerbehebung
- Konfiguration der Optionen „Ausführen als"
- Konfiguration zusätzlicher Einstellungen

Konfiguration von Bereich und Filter

Mit den Einstellungen für Bereich und Filter definieren Sie, wo und wonach die Aktivität suchen soll. Diese Einstellungen werden in der Registerkarte **Suche und Bereich** im Dialogfeld **Eigenschaften der Suchaktivität** konfiguriert.

Gehen Sie zum Konfigurieren der Bereichs- und Filtereinstellungen wie folgt vor:

1. Wählen Sie aus der Liste **Diese Aktivität verwenden, um** die für Ihr Suchszenario geeignete Option:
   - Wählen Sie **In der Organisationseinheit oder im Container suchen** zum Suchen in einer bestimmten OE oder einem Container nach Objekten, die Ihren Suchkriterien entsprechen.
   - Wählen Sie **Nach vom Benutzer oder von der Gruppe verwalteten oder in ihrem Besitz befindlichen Ressourcen suchen** zum Suchen nach den verwalteten Objekten eines bestimmten Benutzers oder einer Gruppe, die Ihren Suchkriterien entsprechen. Verwaltete Objekte eines Benutzers oder einer Gruppe sind jene Objekte, für die der Benutzer oder die Gruppe als primärer oder sekundärer Besitzer festgelegt ist.
   - Wählen Sie **In der Gruppe nach ihren Mitgliedern suchen** zum Suchen nach den Mitgliedern einer bestimmten Gruppe, die Ihren Suchkriterien entsprechen.

- Wählen Sie **Nach direkt Unterstellten des Benutzers suchen** zum Suchen nach den direkt einem bestimmten Benutzer unterstellten Mitarbeitern, die Ihren Suchkriterien entsprechen. Mit den Benutzern direkter Berichte sind jene Benutzer gemeint, für die dieser Benutzer der Verwalter ist.
- Wählen Sie **Suche innerhalb der Objektattribute (ASQ-Suche)** zum Suchen nach den Objekten in einem bestimmten Attribut eines bestimmten Objekts, die Ihren Suchkriterien entsprechen.

2. Wählen Sie in der Liste **Suchen** den Typ des zu suchenden Objekts.

   In Abhängigkeit vom Suchszenario stehen folgende Objekttypen zur Verfügung:

   - **Benutzer.** Zum Suchen nach Benutzerkonten.
   - **Kontakte.** Zum Suchen nach Kontaktobjekten.
   - **Gruppen.** Zum Suchen nach Gruppen.
   - **Computer.** Zum Suchen nach Computerkonten.
   - **Drucker.** Zum Suchen nach Druckerobjekten.
   - **Organisationseinheiten.** Zum Suchen nach Organisationseinheiten.
   - **Freigegebene Ordner.** Zum Suchen nach freigegebenen Ordnern.
   - **Exchange-Empfänger.** Zum Suchen nach Benutzern, Gruppen oder Kontakten mit einem Exchange-Postfach oder einem Exchange-E-Mail-Konto.
   - **Inaktive Konten.** Zum Suchen nach Benutzern/Computern, die sich eine bestimmte Anzahl Tage nicht angemeldet haben oder deren Passwort eine bestimmte Anzahl Tage alt oder abgelaufen ist.
   - **Alle Objekte.** Zum Suchen nach Objekten eines beliebigen Typs.

   Einige Objekttypen sind für bestimmte Suchszenariooptionen nicht verfügbar. Beispiel: Bei der Option zum Suchen nach direkt Unterstellten ist nur **Benutzer** und **Alle Objekte** verfügbar. Unter dem Thema Objekttyp können Sie nachlesen, welche Objekttypen für eine bestimmte Suchszenariooption verfügbar sind.

3. Klicken Sie in das Feld **In**, um festzulegen, wo die Aktivität suchen soll.

   Die Rolle des im Feld **In** konfigurierten Objekts ist von der Suchszenariooption abhängig:

   - Mit **In der Organisationseinheit oder im Container suchen** sucht die Aktivität nach der im Feld **In** angegebenen OE oder dem Container.
   - Mit **Nach vom Benutzer oder von der Gruppe verwalteten oder in ihrem Besitz befindlichen Ressourcen suchen** sucht die Aktivität nach verwalteten Objekten des im Feld **In** angegebenen Benutzer oder der Gruppe.
   - Mit **In der Gruppe nach ihren Mitgliedern suchen** sucht die Aktivität nach Mitgliedern der im Feld **In** angegebenen Gruppe.
   - Mit **Nach direkt Unterstellten des Benutzers suchen** sucht die Aktivität nach direkt unterstellten Mitarbeitern des im Feld **In** angegebenen Benutzers.
   - Mit **Suche innerhalb der Objektattribute (ASQ-Suche)** sucht die Aktivität nach Objekten in einem bestimmten Attribut des im Feld **In** angegebenen Objekts. Sie können das zu suchende Attribut auswählen.

Beim Klicken in das Feld **In** bietet der Workflow Designer eine Reihe von Optionen zum Festlegen des gewünschten Objekts an. In Abhängigkeit vom Suchszenario stehen folgende Optionen zur Verfügung:

SUCHSZENARIO	ZIELOPTION FÜR SUCHE
In der Organisationseinheit oder im Container suchen	• **Fester Container in Verzeichnis.** Sucht in der jeweiligen Organisationseinheit bzw. im jeweiligen Container. Sie können die gewünschte Organisationseinheit bzw. den Container in Active Directory bei der Konfiguration einer Suchaktivität wählen. • **Übergeordnete Organisationseinheit des Arbeitsablaufzielobjekts.** Sucht in der Organisationseinheit, welche das Zielobjekt der Anforderung enthält, die den Arbeitsablauf gestartet hat. • **Vom Arbeitsablaufparameter erkanntes Objekt.** Sucht in der Organisationseinheit oder im Container, die bzw. der durch den Wert eines bestimmten Arbeitsablaufparameters angegeben wurde. Sie können den gewünschten Parameter bei der Konfiguration einer Suchaktivität auswählen. • **Objektes aus Arbeitsablauf-Datenkontext.** Sucht in der Organisationseinheit oder im Container, die bzw. der von der Suchaktivität auf Basis der zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefundenen Daten ausgewählt wird. Bei der Konfiguration einer Suchaktivität können Sie angeben, welche Organisationseinheit bzw. welcher Container von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll. • **Durch Regel-Ausdruck des DN-Werts identifiziertes Objekt.** Sucht in der Organisationseinheit oder im Container, deren bzw. dessen eindeutiger Name (Distinguished Name, DN) vom Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben wird. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration einer Suchaktivität erstellen.
Nach vom Benutzer oder von der Gruppe verwaltete oder in ihrem Besitz befindlichen Ressourcen suchen	• **Arbeitsablaufzielobjekt.** Sucht nach Ressourcen, die vom Zielobjekt der Anforderung, die den Arbeitsablauf gestartet hat, verwaltet bzw. besessen werden. • **Vom Arbeitsablaufparameter erkanntes Objekt.** Sucht nach Ressourcen, die vom Objekt verwaltet oder besessen werden, welches durch den Wert eines bestimmten Arbeitsablaufsparameters angegeben wurde. Sie können den gewünschten Parameter bei der Konfiguration einer Suchaktivität auswählen. • **Objekt aus Arbeitsablauf-Datenkontext.** Sucht nach Ressourcen, die vom Objekt verwaltet oder besessen werden, welches durch die Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt wird. Bei der Konfiguration einer Suchaktivität können Sie angeben, welches Objekt von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll. • **Durch Regel-Ausdruck des DN-Werts identifiziertes Objekt.** Sucht nach Ressourcen, die vom Objekt verwaltet oder besessen werden, dessen eindeutiger Name (Distinguished Name, DN) vom Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben wird. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration einer Suchaktivität erstellen.

SUCHSZENARIO	ZIELOPTION FÜR SUCHE
In der Gruppe nach ihren Mitgliedern suchen	• **Arbeitsablaufzielobjekt.** Sucht nach Mitgliedern der Gruppe, die das Zielobjekt der Anforderung ist, die den Arbeitsablauf gestartet hat. • **Vom Arbeitsablaufparameter erkanntes Objekt.** Sucht in der Gruppe, die vom Wert eines bestimmten Arbeitsablaufparameters angegeben wird. Sie können den gewünschten Parameter bei der Konfiguration einer Suchaktivität auswählen. • **Objekt aus Arbeitsablauf-Datenkontext.** Sucht nach Mitgliedern des Gruppenobjekts, welches durch die Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt wird. Bei der Konfiguration einer Suchaktivität können Sie angeben, welches Gruppenobjekt von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll. • **Durch Regel-Ausdruck des DN-Werts identifiziertes Objekt.** Sucht in der Gruppen, deren eindeutiger Name (Distinguished Name, DN) vom Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben wird. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration einer Suchaktivität erstellen.
Nach direkt Unterstellten des Benutzers suchen	• **Arbeitsablaufzielobjekt.** Sucht nach direkten Berichten des Zielobjekts der Anforderung, die den Arbeitsablauf gestartet hat. • **Vom Arbeitsablaufparameter erkanntes Objekt.** Sucht nach direkten Berichten des Objekts welches durch den Wert eines bestimmten Arbeitsablaufsparameters angegeben wurde. Sie können den gewünschten Parameter bei der Konfiguration einer Suchaktivität auswählen. • **Objekt aus Arbeitsablauf-Datenkontext.** Sucht nach direkten Berichten des Objekts, welches durch die Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt wird. Bei der Konfiguration einer Suchaktivität können Sie angeben, welches Objekt von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll. • **Durch Regel-Ausdruck des DN-Werts identifiziertes Objekt.** Sucht nach direkten Berichten des Objekts, dessen eindeutiger Name (Distinguished Name, DN) vom Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben wird. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration einer Suchaktivität erstellen.
Suche innerhalb der Objektattribute (ASQ-Suche)	• **Festes Objekt im Verzeichnis.** Sucht innerhalb eines bestimmten Attributs des angegebenen Objekts. Sie können das gewünschte Objekt in Active Directory bei der Konfiguration einer Suchaktivität wählen. • **Arbeitsablaufzielobjekt.** Sucht innerhalb eines bestimmten Attributs des Zielobjekts der Anforderung, die den Arbeitsablauf gestartet hat. • **Objekt aus Arbeitsablauf-Datenkontext.** Sucht innerhalb eines bestimmten Attributs des Objekts, welches durch die Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt wird. Bei der Konfiguration einer Suchaktivität können Sie angeben, welches Objekt von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll.

4. Wählen Sie entsprechende Option, um die Suche zu verfeinern.

   Wenn Sie in einer Organisationseinheit oder einem Container suchen, wählen Sie unter **Bei der Suche in der Organisationseinheit oder dem Container** eine der folgenden Optionen:

   - **Nur direkt untergeordnete Objekte der Organisationseinheit oder des Containers abrufen.** Zum Begrenzen der Suche auf Objekte, denen die OE oder der Container in Active Directory direkt übergeordnet ist.
   - **Jedes beliebige Objekt aus der Organisationseinheit oder dem Container abrufen.** Zum Suchen in der gesamten Verzeichnisstruktur, die ihre Basis in der OE oder dem Container hat.

   Wenn Sie nach Ressourcen suchen, von einem bestimmten Benutzer oder einer Gruppe verwaltet werden bzw. sich in deren Besitz befinden, wählen Sie unter **Bei der Suche nach verwalteten Ressourcen** eine oder mehrere der folgenden Optionen:

   - **Vom Benutzer oder der Gruppe (primärer Besitzer) verwaltete Objekte.** Zum Suchen nach Objekten, für die in der Eigenschaft „Verwaltet von" der Benutzer oder die Gruppe angegeben ist.
   - **Objekte abrufen, bei welchen der Benutzer oder die Gruppe ein sekundärer Besitzer ist.** Zum Suchen nach Objekten, für die in der Eigenschaft „Sekundäre Besitzer" der Benutzer oder die Gruppe angegeben ist.
   - **Aufgrund der Mitgliedschaft in Gruppen (indirekte Besitzerschaft) verwaltete oder im Besitz befindliche Objekte abrufen.** Zum Suchen nach Objekten, bei denen der Benutzer oder die Gruppe ein direktes oder indirektes Mitglied der mit der Eigenschaft „Verwaltet von" oder „Sekundärer Besitzer" Gruppe ist.

   Wenn Sie nach Mitgliedern einer bestimmten Gruppe suchen, wählen Sie unter **Bei der Suche in der Gruppe nach ihren Mitgliedern** eine oder mehrere der folgenden Optionen:

   - **Auch indirekte Mitglieder abrufen.** Hiermit werden bei den Suchergebnissen auch indirekte Mitglieder der Gruppe berücksichtigt. Mit dieser Option sucht die Aktivität nicht nur nach Objekte, die direkt zur Gruppe hinzugefügt wurden (direkte Mitglieder), sondern auch nach indirekten Mitgliedern - Objekte, die aufgrund ihrer Mitgliedschaft in anderen Gruppen, die direkte oder indirekte Mitglieder der jeweiligen Gruppe sind, zur Gruppe gehören.
   - **Auch ausstehende Mitglieder abrufen.** Hiermit werden bei den Suchergebnissen Objekte berücksichtigt, die mithilfe der Funktion „Temporäre Gruppenmitgliedschaften" von ActiveRoles in die Gruppe aufgenommen werden sollen.

   Wenn Sie eine ASQ-Suche durchführen möchten, klicken Sie zum Auswählen des Attributs für diese Suche in das Feld **Mit diesem Attribut suchen**. Dies muss ein Attribut sein, das eindeutige Namen (Distinguished Names) speichert, wie etwa das Attribut „Mitglied von" oder „Verwaltet von". Die Suche wird unter den Objekten durchgeführt, die durch die im Attribut gefundenen eindeutigen Namen gekennzeichnet sind. Zum Beispiel sucht eine Suche innerhalb des Attributs „Mitglied von" eines Benutzerkontos nach Gruppen, in denen der Benutzer Mitglied ist.

5. Klicken Sie in das Feld **Suchoptionen**, um die Suche auf Objekte mit bestimmten Merkmalen zu beschränken. Die verfügbaren Suchoptionen sind vom gesuchten Objekttyp abhängig.

   Bei der Suche nach Benutzern:

   - Klicken Sie auf den Hyperlink unter **Nur diese Exchange-Empfänger abrufen**, um die Suche auf Microsoft Exchange-Benutzer mit einem Exchange-Postfach oder einem Exchange-E-Mail-Konto zu beschränken.
   - Klicken Sie auf den Hyperlink unter **Nur inaktive Benutzerkonten abrufen**, um die Suche auf Benutzerkonten zu beschränken, die bestimmte Inaktivitätsbedingungen erfüllen. Im daraufhin angezeigten Dialogfeld können Sie die entsprechenden Inaktivitätsbedingungen wählen.

Bei der Suche nach Kontakten:

- Klicken Sie auf den Hyperlink unter **Nur diese Exchange-Empfänger abrufen**, um die Suche auf Kontakte mit einem E-Mail-Konto mit von Microsoft Exchange zu beschränken.

Bei der Suche nach Gruppen:

- Klicken Sie auf den Hyperlink unter **Nur diese Exchange-Empfänger abrufen**, um die Suche auf Gruppen mit einem E-Mail-Konto mit von Microsoft Exchange zu beschränken.
- Klicken Sie auf den Hyperlink unter **Nur diese Gruppentypen abrufen**, um die Suche auf Gruppen zu beschränken, die bestimmte Bedingungen erfüllen, beispielsweise Gruppen einer bestimmten Art und eines bestimmten Bereichs, leere Gruppen, deprovisionierte Gruppen oder von ActiveRoles kontrollierte Gruppen. Im daraufhin angezeigten Dialogfeld können Sie die entsprechenden Bedingungen für Gruppen wählen.

Bei der Suche nach Computern:

- Klicken Sie auf den Hyperlink unter **Computer mit dieser Rolle abrufen**, um die Suche auf Workstations oder Server oder Domänencontroller zu beschränken.
- Klicken Sie auf den Hyperlink unter **Nur inaktive Computerkonten abrufen**, um die Suche auf Computerkonten zu beschränken, die bestimmte Inaktivitätsbedingungen erfüllen. Im daraufhin angezeigten Dialogfeld können Sie die entsprechenden Inaktivitätsbedingungen wählen.

Bei der Suche nach Druckern:

- Klicken Sie auf die Hyperlinks unter **Nur Drucker mit diesen Funktionen abrufen**, um die Suche auf Drucker mit bestimmten Funktionen wie beispielsweise Druckermodell, Papierformat, Druckauflösung und -geschwindigkeit und andere Funktionen wie beispielsweise doppelseitiges oder farbiges Drucken oder mit Heftfunktion zu beschränken. Im daraufhin angezeigten Dialogfeld können Sie die entsprechenden Druckerfunktionen wählen.

Bei der Suche nach Exchange-Empfängern:

- Klicken Sie auf den Hyperlink unter **Nur diese Exchange-Empfänger abrufen**, um die Suche auf Empfänger zu beschränken, die bestimmte Bedingungen erfüllen, beispielsweise Benutzer mit Exchange-Postfach, mit externer-E-Mail-Adresse, Gruppen mit Exchange-E-Mail-Konto, Kontakte mit externer E-Mail-Adresse, öffentliche Ordner mit Exchange-E-Mail-Konto, abfragebasierte Verteilergruppen, Raum- oder Gerätepostfächer oder verknüpfte oder gemeinsam genutzte Postfächer. Im daraufhin angezeigten Dialogfeld können Sie die entsprechenden Bedingungen für Exchange-Empfänger wählen.
- Klicken Sie auf den Hyperlink unter **Mit diesem Speicherfilter übereinstimmende Postfächer abrufen**, um die Suche auf Postfächer zu beschränken, die auf einem bestimmten Postfachserver gehostet oder in einer bestimmten Postfachdatenbank geführt werden. Im daraufhin angezeigten Dialogfeld können Sie den gewünschten Server bzw. die Datenbank wählen.

Klicken Sie bei der Suche nach inaktiven Konten auf einen Hyperlink unter **Diese Kontotypen abrufen** oder **Konten abrufen, die eine der gewählten Bedingungen erfüllen**; danach lassen Sie im angezeigten Dialogfeld die folgenden Suchoptionen für inaktive Konten anzeigen bzw. ändern Sie sie:

- Wählen Sie unter **Diese Kontotypen abrufen** die gewünschte Option in Abhängigkeit davon, ob Sie nach inaktiven Benutzer- und/oder Computerkonten suchen möchten.
- Unter **Konten abrufen, die eine der gewählten Bedingungen erfüllen** wählen und konfigurieren Sie die Bedingungen für inaktive Konten. Konten, die eine der mehrere von Ihnen gewählte Bedingungen erfüllen, gelten als inaktiv. Die folgenden Bedingungsoptionen sind verfügbar:

Für das Konto liegt keine Anmeldung vor seit <*Zahl*> Tagen. Mit dieser Option können Sie die Zeit (in Tagen) angeben, in denen keine Anmeldung auf diesem Konto erfolgte; nach dieser Zeit gilt das Konto als inaktiv. Die Suche ruft ein bestimmtes Konto ab, wenn für dieses Konto länger als für die mit dieser Option angegebene Anzahl von Tagen keine erfolgreiche Anmeldung verzeichnet wurde.

Die Suchaktivität verwendet das Attribut „lastLogonTimeStamp" um den Zeitpunkt festzustellen, an dem ein bestimmter Benutzer oder Computer sich zuletzt erfolgreich angemeldet hat. Active Directory aktualisiert dieses Attribut nur periodisch und nicht jedes Mal, wenn sich ein Benutzer oder Computer anmeldet. Normalerweise beträgt die Aktualisierungsperiode 14 Tage. Das bedeutet, dass der Wert von „lastLogonTimeStamp" bis zu 14 Tage ungenau sein kann, der tatsächliche letzte Anmeldezeitpunkt ist also später als „lastLogonTimeStamp". Daher empfiehlt es sich, eine Anmeldungs-Inaktivitätsperiode von mehr als 14 Tagen zu wählen.

Das Passwort des Kontos wurde nicht geändert seit <*Zahl*> Tagen. Mit dieser Option können Sie die Gültigkeitsdauer des Passworts (in Tagen) angeben; nach dieser Zeit gilt ein Konto als inaktiv. Die Suche ruft ein bestimmtes Konto ab, wenn das Kennwort des Kontos länger als für die mit dieser Option angegebene Anzahl von Tagen unverändert bleibt.

Das Konto ist abgelaufen seit bisher über <*Zahl*> Tagen. Mit dieser Option können Sie die Anzahl Tage angeben, nach denen ein abgelaufenes Konto als inaktiv gilt. Die Suche ruft ein bestimmtes Konto ab, wenn das Konto über einen längeren Zeitraum in Tagen den Status „Inaktiv" besitzt, als mit dieser Option angegeben.

6. Optional können Sie einen Filter konfigurieren, mit dem die Suche weiter verfeinert wird. Anweisungen hierzu folgen.

Konfiguration eines Suchfilters

Mit der Suchfilteroption können Sie Ihre Suche verfeinern, um Verzeichnisobjekte auf Basis der Objekteigenschaften (Attribute) ausfindig zu machen. Mit einem Suchfilter können Sie in den Objekteigenschaften nach bestimmten Werten suchen. Damit ist sichergestellt, dass die Suchergebnisse nur die Objekte mit den gewünschten Eigenschaften enthalten.

Ein Suchfilter besteht aus Bedingungen, die mit „Und"- oder „Oder"-Logik kombiniert werden. Jede Bedingung stellt eine bestimmte Anweisung dar, welche die Kriterien angibt, mit denen die Aktivität feststellen soll, ob ein bestimmtes Objekt in den Suchergebnissen einzuschließen ist oder nicht. Der Workflow Designer enthält einen Condition Builder für die Konfiguration von Filterbedingungen; dieser befindet sich im Feld **Suchoptionen** auf der Registerkarte **Bereich und Filter** im Dialogfeld **Eigenschaften der Suchaktivität**.

Bei der Konfiguration eines Suchfilters müssen Sie mindestens eine Bedingung hinzufügen. Standardmäßig wird beim Hinzufügen einer Filterbedingung eine einzelne implizierte Bedingungsgruppe erstellt. Sie können weitere Bedingungsgruppen erstellen, um eine Reihe von Bedingungen zu gruppieren und um gruppierte Bedingungen innerhalb anderer Bedingungsgruppen zu verschachteln.

Eine Bedingungsgruppe enthält eine oder mehrere Bedingungen, die durch denselben logischen Operator miteinander verbunden sind. Durch die Gruppierung von Bedingungen geben Sie an, dass diese Bedingungen als eine Einheit bewertet werden sollen. Der Effekt ist derselbe, als wenn Sie einen Ausdruck in einer mathematischen Gleichung oder in einer logischen Aussage in Klammern setzen.

Um eine Bedingung in einer Bedingungsgruppe hinzuzufügen

- Klicken Sie im Feld **Suchoptionen** unter **Filter** auf den Namen der Bedingungsgruppe und danach auf **Bedingung hinzufügen**.

  – ODER –

  Klicken Sie auf das Pluszeichen (+) neben dem Namen der Bedingungsgruppe.

Bei Bedarf können Sie eine Bedingung entfernen, indem Sie auf die mit einem **X** gekennzeichnete Schaltfläche **Bedingung löschen** rechts neben dem Listeneintrag für die Bedingung im Feld **Bedingungen** klicken.

Eine Bedingungsgruppe in einer anderen Bedingungsgruppe hinzufügen

- Klicken Sie im Feld **Suchoptionen** unter **Filter** auf denn Namen der Bedingungsgruppe, zeigen Sie auf **Bedingungsgruppe einfügen** und klicken Sie zur Angabe des logischen Operators auf die entsprechende Option:
  - **AND-Gruppe.** Die Bedingungsgruppe wertet zu TRUE aus, wenn alle Bedingungen in der Gruppe TRUE sind.
  - **OR-Gruppe.** Die Bedingungsgruppe wertet zu TRUE aus, wenn jede Bedingung in der Gruppe TRUE ist.
  - **NOT AND-Gruppe.** Die Bedingungsgruppe wertet zu TRUE aus, wenn jede Bedingung zu FALSE wertet.
  - **NOT AND-Gruppe.** Die Bedingungsgruppe wertet zu TRUE aus, wenn jede Bedingung zu FALSE wertet.

Standardmäßig ist AND der logische Operator zwischen den Bedingungen in einer Bedingungsgruppe. Es ist möglich, die logische Verknüpfung durch Konvertieren der Bedingungsgruppe in einen anderen Gruppentyp zu ändern. Klicken Sie auf den Namen der Gruppe, gehen Sie auf **Bedingungsgruppe konvertieren** und klicken Sie auf die der gewünschten logischen Verknüpfung entsprechende Option.

Sie können auch eine gesamte Bedingungsgruppe entfernen, indem Sie auf den Namen der Gruppe und dann auf **Bedingungsgruppe löschen** klicken.

Wenn Sie eine Bedingung in einer Bedingungsgruppe hinzugefügt haben, können Sie mit den folgenden Schritten die Bedingungen konfigurieren.

Eine Bedingung konfigurieren

1. Klicken Sie auf **Zu bewertende Bedingung konfigurieren** und wählen Sie die Eigenschaft, die von der Bedingung bewertet werden soll.
2. Klick Sie bei Bedarf auf den aktuellen Vergleichsoperator und dann auf den Operator, den die Bedingung verwenden soll.

   *Standardmäßig wird eine Bedingung für die Verwendung des **Ist gleich**-Operators konfiguriert. Die verfügbaren Operatoren sind von der in Schritt 1 gewählten Eigenschaft abhängig.*
3. Klicken Sie auf **Wert definieren zum Vergleich mit** und wählen Sie eine Option für die Angabe des gewünschten Vergleichswerts. Die folgenden Optionen sind verfügbar:

OPTION	BESCHREIBUNG
Textzeichenfolge	Eine Literalzeichenkette. Sie können bei der Konfiguration einer Filterbedingung die gewünschte Zeichenfolge eingeben.
Eigenschaft des Arbeitsablaufzielobjekts	Der Wert einer bestimmten Eigenschaft des Zielobjekts der Anforderung, die den Arbeitsablauf gestartet hat. Sie können bei der Konfiguration einer Filterbedingung die gewünschte Eigenschaft wählen. Normalerweise sollte es sich hierbei um eine Eigenschaft in Form eines Zeichenfolgewerts handeln.
Eigenschaft des Arbeitsablaufinitiators	Der Wert einer bestimmten Eigenschaft des Benutzers, dessen Anforderung den Arbeitsablauf gestartet hat. Sie können bei der Konfiguration einer Filterbedingung die gewünschte Eigenschaft wählen. Normalerweise sollte es sich hierbei um eine Eigenschaft in Form eines Zeichenfolgewerts handeln.

OPTION	BESCHREIBUNG
Geänderter Wert der Eigenschaft des Arbeitsablaufzielobjekts	Der Wert, für die Zuweisung zu einer bestimmten Eigenschaft des Zielobjekts der Anforderung, welche den Arbeitsablauf gestartet hat, angefordert wird, welcher die angeforderte Änderung an der Eigenschaft des Zielobjekts darstellt. Sie können bei der Konfiguration einer Filterbedingung die gewünschte Eigenschaft wählen. Normalerweise sollte es sich hierbei um eine Eigenschaft in Form eines Zeichenfolgewerts handeln.
Eigenschaft des Objekts aus dem Arbeitsablaufdatenkontext	Der Wert einer bestimmten Eigenschaft des Objekts, welches durch die Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt wird. Bei der Konfiguration einer Filterbedingung in einer Suchaktivität können Sie die gewünschte Eigenschaft wählen und angeben, welches Objekt von der Aktivität nach Auswertung der Bedingung zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll.
Durch Regel-Ausdruck generierter Wert	Der Zeichenfolgewert eines bestimmten Regel-Ausdrucks. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden.
Festes Objekt im Verzeichnis	Ein bestimmtes Objekt, wie etwa ein Benutzer, eine Gruppe oder ein Computer. Sie können das gewünschte Objekt in Active Directory bei der Konfiguration einer Filterbedingung wählen. Dieser Vergleichswert ist anwendbar auf Filterbedingungen für DN-Wert-Eigenschaften.
Objekt aus dem Arbeitsablaufdatenkontext	Das Objekt, welches durch die Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt wird. Bei der Konfiguration einer Filterbedingung in einer Suchaktivität können Sie angeben, welches Objekt von der Aktivität nach Auswertung der Bedingung zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll. Dieser Vergleichswert ist anwendbar auf Filterbedingungen für DN-Wert-Eigenschaften.
Durch Regel-Ausdruck des DN-Wertes identifiziertes Objekt	Das Objekt, dessen eindeutiger Name (Distinguished Name, DN) vom Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben wird. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration einer Filterbedingung erstellen. Dieser Vergleichswert ist anwendbar auf Filterbedingungen für DN-Wert-Eigenschaften.
Vom Arbeitsablaufparameter erkanntes Objekt	Das Objekt, das durch einen bestimmten Parameterwert angegeben wird. Sie können bei der Konfiguration einer Filterbedingung den gewünschten Parameter wählen. Dieser Vergleichswert ist anwendbar auf Filterbedingungen für DN-Wert-Eigenschaften.
Objekt des Arbeitsablaufinitiators	Das Benutzerkonto des Benutzers, dessen Anforderung den Arbeitsablauf gestartet hat. Dieser Vergleichswert ist anwendbar auf Filterbedingungen für DN-Wert-Eigenschaften.
Arbeitsablaufzielobjekt	Das Zielobjekt der Anforderung, die den Arbeitsablauf gestartet hat. Dieser Vergleichswert ist anwendbar auf Filterbedingungen für DN-Wert-Eigenschaften.
Festes Datum und feste Uhrzeit	Datum und Uhrzeit als Literalwerte. Sie können bei der Konfiguration einer Filterbedingung das gewünschte Datum und die gewünschte Uhrzeit wählen. Dieser Vergleichswert ist anwendbar auf Filterbedingungen für Eigenschaften mit einem Datum/Uhrzeit-Wert.

OPTION	BESCHREIBUNG
Datum und Uhrzeit des Arbeitsablaufs	Ein bestimmter Zeitpunkt relativ zum Datum und zur Uhrzeit der Ausführung der Suchaktivität. Sie haben die Option, ein Datum anzugeben, das eine bestimmte Anzahl von Daten vor oder nach Ausführung der Suchaktivität liegt. Dieser Vergleichswert ist anwendbar auf Filterbedingungen für Eigenschaften mit einem Datum/Uhrzeit-Wert.
Richtig	Der boolesche Literalwert von Wahr.
Falsch	Der boolesche Literalwert von Falsch.
Vom Skript generierter Wert	Der Wert, der von einer bestimmten Skriptfunktion zurückgegeben wird. Sie können bei der Konfiguration einer Filterbedingung die gewünschte Skriptfunktion wählen. Die Suchaktivität wird diese Skriptfunktion nach Auswertung der Bedingung zum Ausführungszeitpunkt des Arbeitsablaufs ausführen.
Arbeitsablaufparameter-wert	Der Wert eines bestimmten Arbeitsablaufsparameters. Sie können bei der Konfiguration einer Filterbedingung den gewünschten Parameter wählen.

Konfiguration einer Benachrichtigung

Sie können eine Suchaktivität darauf konfigurieren, Empfänger als Abonnenten der Benachrichtigungen folgender Ereignisse festzulegen:

- **Aktivität erfolgreich abgeschlossen.** Wenn diese Aktivität so konfiguriert wurde, dass Benachrichtigungen über dieses Ereignis erfolgen, versendet ActiveRoles eine Benachrichtigungs-E-Mail, wenn während der Ausführung dieser Aktivität keine erheblichen Fehler festgestellt wurden.
- **Aktivität hat einen Fehler festgestellt.** Wenn diese Aktivität so konfiguriert wurde, dass Benachrichtigungen über dieses Ereignis erfolgen, versendet ActiveRoles eine Benachrichtigungs-E-Mail, wenn während der Ausführung dieser Aktivität erhebliche Fehler festgestellt wurden.

Gehen Sie zum Konfigurieren einer Benachrichtigung für eine Suchaktivität wie folgt vor:

1. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Suchaktivität und klicken Sie dann auf **Eigenschaften**.
2. Gehen Sie zur Registerkarte **Benachrichtigung** im Dialogfeld **Eigenschaften der Suchaktivität** und konfigurieren Sie die Benachrichtigungseinstellungen mit den Schritten in Konfigurieren einer Benachrichtigungsaktivität.

Die Benachrichtigungseinstellungen geben das Ereignis an, über das eine Benachrichtigung versendet werden soll, sowie die Empfänger der Benachrichtigung. Wenn sie vom Arbeitsablauf ausgeführt wird, verfasst diese Aktivität eine dem angegebenen Ereignis entsprechende Benachrichtigung. ActiveRoles hält die von der Aktivität vorbereitete Meldung zurück und sendet die Meldung bei Eintritt des Ereignisses an die angegebenen Empfänger.

Konfigurieren der Fehlerbehebung

Bei der Konfiguration einer Suchaktivität können Sie die Fehlerbehebung so konfigurieren, dass Fehler, die bei dieser Suchaktivität und allen in dieser Aktivität enthaltenen Aktivitäten festgestellt werden, unterdrückt werden.

Gehen Sie zum Konfigurieren der Fehlerbehebung für eine Suchaktivität wie folgt vor:

1. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Suchaktivität und klicken Sie dann auf **Eigenschaften**.
2. Gehen Sie zur Registerkarte **Fehlerbehebung** im Dialogfeld **Eigenschaften der Suchaktivität** und markieren Sie das Kontrollkästchen **Arbeitsablauf fortsetzen, auch wenn bei dieser Aktivität ein Fehler festgestellt wird** auf dieser Registerkarte bzw. löschen Sie die Markierung.

Wenn **Arbeitsablauf fortsetzen, auch wenn bei dieser Aktivität ein Fehler festgestellt wird** markiert ist (Standardeinstellung), beendet ActiveRoles bei einem bei dieser Aktivität festgestellten Fehler den Arbeitsablauf. Wenn Sie dieses Kontrollkästchen markieren, wird der Arbeitsablauf unabhängig davon fortgesetzt, ob bei der Suchaktivität oder einer darin enthaltenen Aktivität ein Fehler festgestellt wird.

Konfiguration der Optionen „Ausführen als"

Standardmäßig wird die Suchaktivität unter dem Benutzerkonto ausgeführt, das in der Einstellung „Ausführen als" in den Optionen und Startbedingungen des Arbeitsablaufs festgelegt wurde. Dabei kann es sich um das Dienstkonto des ActiveRoles-Verwaltungsdienstes oder um das Konto des Benutzers handeln, der den Start des Arbeitsablaufs ausgelöst hat. Sie können die Aktivität so konfigurieren, dass sie die Standardeinstellung für „Ausführen als" ersetzt.

Gehen Sie zum Konfigurieren von Optionen „Ausführen als" für eine Suchaktivität wie folgt vor:

1. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Suchaktivität und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie auf den Hyperlink **Optionen „Ausführen als"** unten im Dialogfeld **Eigenschaften der Suchaktivität**.
3. Markieren Sie zum Ersetzen der Standardeinstellung „Ausführen als" für diese Aktivität das Kontrollkästchen **Diese Aktivität ausführen unter** und wählen Sie das Konto, unter dem diese Aktivität ausgeführt werden soll:
   - Klicken Sie auf **Das Dienstkonto von Quest One ActiveRoles**, wenn dieser Aktivität unter dem Dienstkonto des ActiveRoles Verwaltungsdiensts ausgeführt werden soll.
   - Klicken Sie auf **Das Konto des Benutzers, der mit dem Arbeitsablauf begonnen hat**, wenn diese Aktivität unter dem Konto des Benutzers ausgeführt werden soll, der den Arbeitsablauf initialisiert hat. In Abhängigkeit vom Arbeitsablauftyp ist dies der Benutzer, der den Vorgang angefragt hat, mit dem der Arbeitsablauf gestartet wurde, oder der Benutzer, der den Arbeitsablauf auf Anfrage gestartet hat.

Das Konto, unter dem die Aktivität ausgeführt wird, bestimmt die Zugriffsrechte der Aktivität im Verzeichnis.

Konfiguration zusätzlicher Einstellungen

Sie können mit einer Reihe weiterer Einstellungen eine Suchaktivität so konfigurieren, dass die Suche endet, wenn die Anzahl der Objekte, die die Suchbedingungen erfüllen, einen bestimmten Grenzwert übersteigt. Darüber hinaus kann das Verhalten einer Suchaktivität mit sog. Anforderungskontrollen beeinflusst werden. Diese Anforderungskontrollen leiten an ActiveRoles zusätzliche Informationen über die Verarbeitung von Vorgangsanfragen weiter, die von dieser Aktivität erstellt wurden.

Gehen Sie zum Konfigurieren zusätzlicher Einstellungen für eine Suchaktivität wie folgt vor:

1. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Suchaktivität und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie auf den Hyperlink **Zusätzliche Einstellungen** unten im Dialogfeld **Eigenschaften der Suchaktivität**.
3. Markieren Sie das Kontrollkästchen **Die Suchaktivität beenden bei Rückgabe von mehr als**, damit die Suchaktivität stoppt, wenn die Anzahl der gefundenen Objekte einen bestimmten Grenzwert übersteigt, und geben Sie die maximale Anzahl Objekte an, die die Aktivität bei einer Suche anzeigen soll.
4. Ändern, löschen oder fügen Sie Anforderungskontrollen in der Liste **Diese Kontrollen in die Aktivitäts-Vorgangsanforderung aufnehmen bzw. davon ausschließen**.

   Klicken Sie zum Hinzufügen oder Änderungen einer Kontrolle auf **Hinzufügen** bzw. **Ändern** und geben Sie im daraufhin angezeigten Dialogfeld den Namen und, sofern vorhanden, den Wert der Kontrolle ein. Wenn die Aktivität die Kontrolle zu den Anforderungen hinzufügen soll, klicken Sie auf **Diese Kontrolle in die Aktivitäts-Vorgangsanforderungen aufnehmen**. Wenn Sie sichergehen möchten, dass die Kontrolle nie in den von dieser Aktivität erstellten Anforderungen erscheint, klicken Sie auf **Diese Kontrolle aus den Aktivitäts-Vorgangsanforderungen ausschließen**.

Anforderungskontrollen sind Daten in einer Vorgangsanforderung, mit denen zusätzliche Informationen über die Verarbeitung der Anforderung an ActiveRoles übermittelt werden. Anforderungskontrollen sind optional. Wenn keine Anforderungskontrollen zu einer Anforderung hinzugefügt werden, bestimmt ActiveRoles allein auf Basis des Anforderungstyps, wie die Anforderung verarbeitet werden soll. Informationen über Anforderungskontrollen finden Sie in Active Roles SDK.

Konfiguration von CRUD-Aktivitäten

ActiveRoles bietet eine Reihe an Arbeitsablauf-Aktivitäten, die gemeinhin als CRUD-Aktivitäten bezeichnet werden und darauf ausgelegt sind, neue Objekte zu erstellen und bestehende Objekte in Active Directory zu modifizieren oder zu löschen. Die CRUD-Abkürzung bezieht sich auf die Hauptvorgänge (in englischer Sprache), die mit diesen Aktivitäten durchgeführt werden können: Erstellen (Create), Lesen (Read), Aktualisieren (Update), Löschen (Delete). Dieser Abschnitt enthält Hinweise zum Konfigurieren der folgenden CRUD-Aktivitäten:

- Aktivität „Erstellen“ Erstellt ein Objekt, z.B. einen Benutzer, eine Gruppe oder einen Computer, in Active Directory.
- Aktivität „Aktualisieren“ Ändert die Eigenschaften eines Objekts, z.B. eines Benutzers, eines Computers oder einer Gruppe, in Active Directory.
- Aktivität „Zu einer Gruppe hinzufügen“ Fügt ein Objekt, z.B. einen Benutzer, eine Gruppe oder einen Computer, in Active Directory hinzu.
- Aktivität „Aus einer Gruppe entfernen“ Entfernt ein Objekt, z.B. einen Benutzer, eine Gruppe oder einen Computer, aus bestimmten Gruppen in Active Directory.
- Aktivität „Verschieben“ Verschiebt ein Objekt, z.B. einen Benutzer, eine Gruppe oder einen Computer, in einen bestimmten Container in Active Directory.

- Aktivität „Deprovisionieren“ Deprovisioniert einen Benutzer oder eine Gruppe durch Anwendung der Deprovisionsrichtlinie von ActiveRoles.
- Aktivität „Deprovisionierung aufheben“ Stellt einen Benutzer oder eine Gruppe wieder her, der bzw. die mit Hilfe von ActiveRoles deprovisioniert wurde.
- Aktivität „Löschen“ Löscht ein Objekt, z.B. einen Benutzer, einen Computer oder eine Gruppe, in Active Directory.

Dieser Abschnitt enthält die Schritte zum Konfigurieren der in den CRUD-Aktivitäten gemeinsamen Einstellungen:

- Konfigurieren von Benachrichtigungen ActiveRoles kann eine E-Mail-Benachrichtigung dazu aussenden, ob die Aktivität zum Ausführungszeitpunkt eine Fehlerbedingung festgestellt hat oder nicht.
- Konfigurieren von Fehlerbehebungen Legt fest, ob der Arbeitsablauf auch dann fortgesetzt werden darf, wenn die Aktivität zum Ausführungszeitpunkt eine Fehlerbedingung festgestellt hat.
- Konfigurieren von „Ausführen als“-Optionen Legt das Konto fest, unter dem die Aktivität ausgeführt werden soll.
- Konfigurieren zusätzlicher Einstellungen Diverse erweiterte Konfigurationsoptionen, mit denen Sie die Verarbeitung des von der Aktivität angeforderten Vorgangs anpassen können.

Aktivität „Erstellen“

Beim Konfigurieren einer Erstellungsaktivität können Sie die Organisationseinheit oder den Container angeben, in der bzw. dem die Aktivität Objekte erstellt, den Objekttyp und -namen wählen und angeben, wie die Aktivität die Eigenschaften der neu erstellten Objekte auffüllen soll. Weitere Optionen sind verfügbar: Benachrichtigung, Fehlerbehebung und Optionen „Ausführen als“.

Gehen Sie folgendermaßen vor, um eine Erstellungsaktivität zu konfigurieren:

1. Erweitern Sie in der Konsolenstruktur von Quest One ActiveRoles **Konfiguration | Richtlinien | Arbeitsablauf** und wählen Sie dann den Arbeitsablauf, der die Erstellungsaktivität enthält, die Sie konfigurieren möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details“ geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.
2. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Aktivität und klicken Sie dann auf **Eigenschaften**.
3. Gehen Sie zur Registerkarte **Container** im Dialogfeld **Eigenschaften der Skriptaktivität**.
4. Klicken Sie zum Angeben der Organisationseinheit (OE) oder des Containers, in dem die Aktivität ein Objekt erstellen soll, in das Feld **Die Aktivität erstellt das Objekt in diesem Container**. Die folgenden Optionen sind verfügbar:
   - **Fester Container im Verzeichnis.** Mit dieser Option erstellt die Aktivität in der angegebenen OE bzw. im Container ein Objekt. Sie können die gewünschte Organisationseinheit bzw. den Container in Active Directory bei der Konfiguration einer Erstellungsaktivität wählen.
   - **Aktivitätszielobjekt.** Mit dieser Option erstellt die Aktivität ein Objekt in der OE bzw. in dem Container, die bzw. der bei der Ausführung des Arbeitsablaufs von einer anderen CRUD-Aktivität erstellt oder in anderer Form verarbeitet wurde. Sie können die gewünschte CRUD-Aktivität bei der Konfiguration einer Erstellungsaktivität aus der Arbeitsablaufdefinition wählen.
   - **Vom Arbeitsablauf erkanntes Objekt.** Mit dieser Option erstellt die Aktivität ein Objekt in der OE bzw. in dem Container, der durch den Wert eines bestimmten Arbeitsablaufparameters angegeben wird. Sie können den gewünschten Parameter bei der Konfiguration einer Erstellungsaktivität aus der Arbeitsablaufdefinition wählen.

- **Objekt aus dem Arbeitsablaufdatenkontext.** Mit dieser Option erstellt die Aktivität ein Objekt in der OE bzw. in dem Container, die bzw. der bei Ausführung des Arbeitsablaufs auf der Basis der in der Arbeitsablaufumgebung festgestellten Daten von der Erstellungsaktivität ausgewählt wird. Bei der Konfiguration einer Erstellungsaktivität können Sie angeben, welche Organisationseinheit bzw. welcher Container von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll.
- **Objekt durch Regelausdruck des DN-Werts identifiziert.** Mit dieser Option erstellt die Aktivität ein Objekt in der OE bzw. in dem Container, dessen Distinguished Name (DN) durch den Zeichenfolgenwert eines bestimmten Regel-Ausdrucks angegeben wird. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration einer Erstellungsaktivität erstellen.

5. Gehen Sie zur Registerkarte **Objektname** im Dialogfeld **Eigenschaften der Skriptaktivität**.
6. Klicken Sie in das Feld **Objekttyp** und wählen Sie den Typ der Objekte, die die Aktivität erstellen soll, beispielsweise Benutzer, Gruppe, Computer usw.
7. Klicken Sie in das Feld **Objektname**, um anzugeben, wie die Aktivität beim Erstellen des Objekts den Objektnamen erzeugen soll. Die folgenden Optionen sind verfügbar:
   - **Textzeichenfolge.** Mit dieser Option nutzt die Aktivität die eingegebene Zeichenfolge als Objektnamen. Sie können die gewünschte Zeichenfolge bei der Konfiguration einer Erstellungsaktivität angeben.
   - **Arbeitsablaufparameterwert.** Mit dieser Option nutzt die Aktivität den durch den Zeichenfolgenwert eines bestimmten Arbeitsablaufparameters angegebenen Namen. Sie können den gewünschten Parameter bei der Konfiguration einer Erstellungsaktivität aus der Arbeitsablaufdefinition wählen.
   - **Eigenschaft des Objekts aus dem Arbeitsablaufdatenkontext.** Mit dieser Option nutzt die Aktivität den Namen, der durch den Wert einer bestimmten Objekteigenschaft angegeben wird. Diese Eigenschaft wird von der Erstellungsaktivität auf der Basis der in der Arbeitsablaufumgebung während der Ausführung des Arbeitsablaufs gefundenen Daten ausgewählt. Bei der Konfiguration einer Erstellungsaktivität können Sie die gewünschte Eigenschaft wählen und angeben, welches Objekt von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll.
   - **Wert durch Regel-Ausdruck generiert.** Mit dieser Option nutzt die Aktivität den durch den Zeichenfolgenwert eines bestimmten Regel-Ausdrucks angegebenen Namen. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration einer Erstellungsaktivität erstellen.
8. Gehen Sie zur Registerkarte **Objekteigenschaften** im Dialogfeld **Eigenschaften der Aktivität „Erstellen"**.
9. Gehen Sie zum Konfigurieren der von der Aktivität aufzufüllenden Eigenschaftsliste wie folgt vor:
   - Klicken Sie zum Hinzufügen einer Eigenschaft zur Liste auf **Eigenschaft hinzufügen** und wählen Sie den Namen der gewünschten Eigenschaft aus.
   - Klicken Sie zum Löschen einer Eigenschaft aus der Liste auf die mit **X** markierte **Löschtaste** rechts neben dem Listeneintrag für diese Eigenschaft.

10. Nach dem Hinzufügen einer Eigenschaft zur Liste klicken Sie in das Feld **Wert**, um den Wert anzugeben, den die Aktivität dieser Eigenschaft des neu erstellten Objekts zuweisen soll. Die folgenden Optionen sind verfügbar:
    - **Textzeichenfolge.** Mit dieser Option weist die Aktivität die eingegebene Zeichenfolge der Eigenschaft zu. Sie können die gewünschte Zeichenfolge bei der Konfiguration einer Erstellungsaktivität angeben.
    - **Eigenschaft des Arbeitsablaufinitiators.** Mit dieser Option füllt die Aktivität die Eigenschaft mit dem Wert einer bestimmten Eigenschaft des Benutzers auf, dessen Anfrage den Arbeitsablauf gestartet hat. Sie können die gewünschte Eigenschaft bei der Konfiguration einer Erstellungsaktivität angeben.
    - **Arbeitsablaufparameterwert.** Mit dieser Option füllt die Aktivität die Eigenschaft mit dem Wert eines bestimmten Arbeitsablaufparameters auf. Sie können den gewünschten Parameter bei der Konfiguration einer Erstellungsaktivität aus der Arbeitsablaufdefinition wählen.
    - **Eigenschaft des Objekts aus dem Arbeitsablaufdatenkontext.** Mit dieser Option füllt die Aktivität die Eigenschaft mit dem Wert einer bestimmten Eigenschaft des Objekts auf. Diese Eigenschaft wird von der Erstellungsaktivität auf der Basis der in der Arbeitsablaufumgebung während der Ausführung des Arbeitsablaufs gefundenen Daten ausgewählt. Bei der Konfiguration einer Erstellungsaktivität können Sie die gewünschte Eigenschaft wählen und angeben, welches Objekt von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll.
    - **Wert durch Regel-Ausdruck generiert.** Mit dieser Option füllt die Aktivität die Eigenschaft mit dem Zeichenfolgenwert eines bestimmten Regel-Ausdrucks auf. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration einer Erstellungsaktivität erstellen.
11. Lassen Sie Benachrichtigungseinstellungen anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von Benachrichtigungen.
12. Lassen Sie Einstellungen für Fehlerbehebung anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von Fehlerbehebungen.
13. Lassen Sie Optionen „Ausführen als" anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von „Ausführen als"-Optionen.
14. Lassen Sie erweiterte Einstellungen anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren zusätzlicher Einstellungen.

Aktivität „Aktualisieren"

Bei der Konfiguration einer Aktualisierungsaktivität können Sie die Regeln für die Auswahl des Objekts angeben, dessen Eigenschaften von der Aktivität geändert werden sollen, und festlegen, wie die Aktivität die Eigenschaften des Objekts ändern soll. Weitere Optionen sind verfügbar: Benachrichtigung, Fehlerbehebung und Optionen „Ausführen als".

Gehen Sie zum Konfigurieren einer Aktualisierungsaktivität wie folgt vor:

1. Erweitern Sie in der Konsolenstruktur von Quest One ActiveRoles **Konfiguration | Richtlinien | Arbeitsablauf** und wählen Sie dann den Arbeitsablauf, der die Aktualisierungsaktivität enthält, die Sie konfigurieren möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.

2. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Aktivität und klicken Sie dann auf **Eigenschaften**.

3. Gehen Sie zur Registerkarte **Aktivitätsziel** im Dialogfeld **Eigenschaften der Aktivität „Aktualisieren"**.
4. Klicken Sie in das Feld **Die Aktivität führt den Vorgang an diesem Objekt aus**, um das Objekt anzugeben, dessen Eigenschaften durch die Aktivität geändert werden sollen. Dieses Objekt wird als Aktivitätsziel bezeichnet. Sie können das Aktivitätsziel mit den folgenden Optionen angeben:
   - **Festes Objekt im Verzeichnis.** Das Aktivitätsziel ist das angegebene Objekt. Sie können das gewünschte Objekt bei der Konfiguration der Aktualisierungsaktivität in Active Directory auswählen.
   - **Vom Arbeitsablaufparameter erkanntes Objekt.** Das Aktivitätsziel ist das Objekt, welches durch den Wert eines bestimmten Arbeitsablaufsparameters angegeben wurde. Sie können den gewünschten Parameter bei der Konfiguration der Aktualisierungsaktivität aus der Arbeitsablaufdefinition auswählen.
   - **Objekt aus Arbeitsablauf-Datenkontext.** Das Aktivitätsziel wird von der Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt. Bei der Konfiguration der Aktualisierungsaktivität können Sie angeben, welches Objekt von der Aktivität bei der Ausführung des Arbeitsablaufs ausgewählt werden soll.
   - **Durch Regel-Ausdruck des DN-Wertes identifiziertes Objekt.** Der eindeutige Name (Distinguished Name, DN) des Aktivitätsziels wird durch den Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration der Aktualisierungsaktivität erstellen.
5. Gehen Sie zur Registerkarte **Zieleigenschaften** im Dialogfeld **Eigenschaften der Aktivität „Aktualisieren"**.
6. Gehen Sie zum Konfigurieren der von der Aktivität zu verändernden Eigenschaftsliste wie folgt vor:
   - Klicken Sie zum Hinzufügen einer Eigenschaft zur Liste auf **Eigenschaft hinzufügen** und wählen Sie den Namen der gewünschten Eigenschaft aus.
   - Klicken Sie zum Löschen einer Eigenschaft aus der Liste auf die mit **X** markierte **Löschtaste** rechts neben dem Listeneintrag für diese Eigenschaft.
7. Klicken Sie nach dem Hinzufügen einer Eigenschaft in das Feld **Aktion**, um die Art der Änderungen anzugeben, die die Aktivität an dieser Eigenschaft vornehmen soll:
   - Klicken Sie auf **Einstellen**, damit die Aktivität der Eigenschaft einen neuen Wert zuweist.
   - Klicken Sie auf **Löschen**, damit die Aktivität diese Eigenschaft vom Objekt entfernt.
   - Klicken Sie bei einer Eigenschaft mit mehreren Werten auf **Wert hinzufügen** oder **Wert entfernen**, damit die Aktivität den Wert zur Eigenschaft hinzufügt bzw. davon entfernt.
8. Wenn im Feld **Aktion** eine andere Aktion als **Löschen** ausgewählt ist, klicken Sie in das Feld **Wert**, um den Eigenschaftswert anzugeben, den die Aktivität festlegen, hinzufügen oder entfernen soll. Die folgenden Optionen sind verfügbar:
   - **Textzeichenfolge.** Verwendet die angegebene Zeichenfolge als Wert der Eigenschaft. Sie können die gewünschten Zeichenfolge bei der Konfiguration der Aktualisierungsaktivität erstellen.
   - **Eigenschaft des Arbeitsablaufsinitiators.** Verwendet den Wert einer bestimmten Eigenschaft des Benutzers, dessen Anforderung den Arbeitsablauf gestartet hat. Sie können die gewünschten Eigenschaft bei der Konfiguration der Aktualisierungsaktivität auswählen.

- **Arbeitsablaufparameterwert.** Verwendet den Wert eines bestimmten Arbeitsablaufsparameters. Sie können den gewünschten Parameter bei der Konfiguration der Aktualisierungsaktivität aus der Arbeitsablaufdefinition auswählen.
- **Eigenschaft des Objektes aus dem Arbeitsablauf-Datenkontext.** Verwendet den Wert einer bestimmten Eigenschaft jenes Objekts, das von der Aktualisierungsaktivität auf Basis der zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefundenen Daten ausgewählt wird. Bei der Konfiguration der Aktualisierungsaktivität können Sie die gewünschte Eigenschaft auswählen und angeben, welches Objekt von der Aktivität bei der Ausführung des Arbeitsablaufs ausgewählt werden soll.
- **Durch Regel-Ausdruck generierter Wert.** Verwendet den Zeichenfolgewert eines bestimmten Regel-Ausdrucks. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration einer Aktualisierungsaktivität erstellen.

9. Lassen Sie Benachrichtigungseinstellungen anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von Benachrichtigungen.
10. Lassen Sie Einstellungen für Fehlerbehebung anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von Fehlerbehebungen.
11. Lassen Sie Optionen „Ausführen als" anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von „Ausführen als"-Optionen.
12. Lassen Sie erweiterte Einstellungen anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren zusätzlicher Einstellungen.

Aktivität „Zu einer Gruppe hinzufügen"

Beim Konfigurieren einer Aktivität „Zu einer Gruppe hinzufügen" können Sie die Regeln für die Auswahl des Objekts festlegen, das die Aktivität zu Gruppen hinzufügen soll, und die Gruppen definieren, zu denen die Aktivität das Objekt hinzufügen soll. Weitere Optionen sind verfügbar: Benachrichtigung, Fehlerbehebung und Optionen „Ausführen als".

Gehen Sie zum Konfigurieren einer Aktivität „Zu einer Gruppe hinzufügen" wie folgt vor:

1. Erweitern Sie in der Konsolenstruktur von Quest One ActiveRoles **Konfiguration | Richtlinien | Arbeitsablauf** und wählen Sie dann den Arbeitsablauf, der die Aktivität „Zu einer Gruppe hinzufügen" enthält, die Sie konfigurieren möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.

2. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Aktivität und klicken Sie dann auf **Eigenschaften**.
3. Gehen Sie zur Registerkarte **Aktivitätsziel** im Dialogfeld **Eigenschaften der Aktivität „Zu einer Gruppe hinzufügen"**.
4. Klicken Sie in das Feld **Die Aktivität führt den Vorgang an diesem Objekt aus**, um das Objekt anzugeben, das die Aktivität zu Gruppen hinzufügen soll. Dieses Objekt wird als Aktivitätsziel bezeichnet. Sie können das Aktivitätsziel mit den folgenden Optionen angeben:
   - **Festes Objekt im Verzeichnis.** Das Aktivitätsziel ist das angegebene Objekt. Sie können das gewünschte Objekt bei der Konfiguration der Aktivität „Zu einer Gruppe hinzufügen" in Active Directory auswählen.
   - **Vom Arbeitsablaufparameter erkanntes Objekt.** Das Aktivitätsziel ist das Objekt, welches durch den Wert eines bestimmten Arbeitsablaufsparameters angegeben wurde. Sie können den gewünschten Parameter bei der Konfiguration der Aktivität „Zu einer Gruppe hinzufügen" aus der Arbeitsablaufdefinition auswählen.

- **Objekt aus Arbeitsablauf-Datenkontext.** Das Aktivitätsziel wird von der Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt. Bei der Konfiguration der Aktivität „Zu einer Gruppe hinzufügen" können Sie angeben, welches Objekt von der Aktivität bei der Ausführung des Arbeitsablaufs ausgewählt werden soll.
- **Durch Regel-Ausdruck des DN-Wertes identifiziertes Objekt.** Der eindeutige Name (Distinguished Name, DN) des Aktivitätsziels wird durch den Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration der Aktivität „Zu einer Gruppe hinzufügen" erstellen.

5. Gehen Sie zur Registerkarte **Gruppen** im Dialogfeld **Eigenschaften der Aktivität „Zu einer Gruppe hinzufügen"**.
6. Konfigurieren Sie die Liste der Gruppen, zu denen die Aktivität das Zielobjekt hinzufügen soll.

   Klicken Sie zum Hinzufügen einer Gruppe zur Liste auf **Gruppe hinzufügen** und wählen sie eine der folgenden Optionen aus:

   - **Feste Gruppe in Verzeichnis.** Sie können die gewünschte Gruppe bei der Konfiguration der Aktivität „Zu einer Gruppe hinzufügen" in Active Directory auswählen. Ein eindeutiger Kennzeichner der Gruppe wird in der Konfiguration der Aktivität gespeichert. Die Aktivität verwendet diesen Kennzeichner, um die Gruppe bei der Berechnung der Gruppenliste zum Ausführungszeitpunkt des Arbeitsablaufs auszuwählen.
   - **Objekt aus Arbeitsablauf-Datenkontext.** Die Gruppe wird von der Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt. Bei der Konfiguration der Aktivität „Zu einer Gruppe hinzufügen" können Sie angeben, welche Gruppe von der Aktivität bei der Ausführung des Arbeitsablaufs ausgewählt werden soll.
   - **Durch Regel-Ausdruck des DN-Wertes identifiziertes Objekt.** Der eindeutige Name (Distinguished Name, DN) der Gruppe wird durch den Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration der Aktivität „Zu einer Gruppe hinzufügen" erstellen.

   Klicken Sie zum Löschen einer Gruppe aus der Liste auf die mit **X** markierte **Löschtaste** rechts neben dem Listeneintrag für diese Gruppe.

7. Lassen Sie Benachrichtigungseinstellungen anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von Benachrichtigungen.
8. Lassen Sie Einstellungen für Fehlerbehebung anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von Fehlerbehebungen.
9. Lassen Sie Optionen „Ausführen als" anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von „Ausführen als"-Optionen.
10. Lassen Sie erweiterte Einstellungen anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren zusätzlicher Einstellungen.

Aktivität „Aus einer Gruppe entfernen"

Beim Konfigurieren einer Aktivität „Aus einer Gruppe entfernen" können Sie die Regeln für die Auswahl des Objekts festlegen, das die Aktivität aus Gruppen entfernen soll, und die Gruppen definieren, aus denen die Aktivität das Objekt entfernen soll. Weitere Optionen sind verfügbar: Benachrichtigung, Fehlerbehebung und Optionen „Ausführen als".

Gehen Sie zum Konfigurieren einer Aktivität „Aus einer Gruppe entfernen" wie folgt vor:

1. Erweitern Sie in der Konsolenstruktur von Quest One ActiveRoles **Konfiguration | Richtlinien | Arbeitsablauf** und wählen Sie dann den Arbeitsablauf, der die Aktivität „Aus einer Gruppe entfernen" enthält, die Sie konfigurieren möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.

2. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Aktivität und klicken Sie dann auf **Eigenschaften**.
3. Gehen Sie zur Registerkarte **Aktivitätsziel** im Dialogfeld **Eigenschaften der Aktivität „Aus einer Gruppe entfernen"**.
4. Klicken Sie in das Feld **Die Aktivität führt den Vorgang an diesem Objekt aus**, um das Objekt anzugeben, das die Aktivität aus Gruppen entfernen soll. Dieses Objekt wird als Aktivitätsziel bezeichnet. Sie können das Aktivitätsziel mit den folgenden Optionen angeben:
   - **Festes Objekt im Verzeichnis.** Das Aktivitätsziel ist das angegebene Objekt. Sie können das gewünschte Objekt bei der Konfiguration der Aktivität „Aus einer Gruppe entfernen" in Active Directory auswählen.
   - **Vom Arbeitsablaufparameter erkanntes Objekt.** Das Aktivitätsziel ist das Objekt, welches durch den Wert eines bestimmten Arbeitsablaufsparameters angegeben wurde. Sie können den gewünschten Parameter bei der Konfiguration der Aktivität „Aus einer Gruppe entfernen" aus der Arbeitsablaufdefinition auswählen.
   - **Objekt aus Arbeitsablauf-Datenkontext.** Das Aktivitätsziel wird von der Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt. Bei der Konfiguration der Aktivität „Aus einer Gruppe entfernen" können Sie angeben, welches Objekt von der Aktivität bei der Ausführung des Arbeitsablaufs ausgewählt werden soll.
   - **Durch Regel-Ausdruck des DN-Wertes identifiziertes Objekt.** Der eindeutige Name (Distinguished Name, DN) des Aktivitätsziels wird durch den Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration der Aktivität „Aus einer Gruppe entfernen" erstellen.
5. Gehen Sie zur Registerkarte **Gruppen** im Dialogfeld **Eigenschaften der Aktivität „Aus einer Gruppe entfernen"**.
6. Wählen Sie unter diesen Optionen aus:
   - **Das Objekt aus allen Gruppen entfernen.** Mit dieser Option wird die Aktivität so konfiguriert, dass sie das Objekt aus allen Gruppen in Active Directory entfernt. Ein Objekt kann nicht aus seiner primären Gruppe entfernt werden; daher wird mit dieser Aktivität das Objekt aus allen Gruppen außer seiner primären Gruppe entfernt.
   - **Objekt aus diesen Gruppen entfernen.** Mit dieser Option können Sie die Gruppen auflisten, aus denen die Aktivität das Objekt entfernen soll. Sie können bei der Konfiguration einer Aktivität „Aus Gruppe entfernen" eine Liste von Gruppen angeben. Die Aktivität wird das Objekt aus jeder in der Liste aufgeführten Gruppe (außer aus der primären Gruppe des Objekts) entfernen.

7. Wenn Sie die Option **Objekt aus diesen Gruppen entfernen** gewählt haben, konfigurieren Sie die Liste der Gruppen, aus denen die Aktivität das Objekt entfernen soll. Klicken Sie zum Hinzufügen einer Gruppe zur Liste auf **Gruppe hinzufügen** und wählen sie eine der folgenden Optionen aus:
   - **Feste Gruppe im Verzeichnis.** Sie können die gewünschte Gruppe bei der Konfiguration einer Aktivität „Aus Gruppe entfernen" in Active Directory wählen. Ein eindeutiger Kennzeichner der Gruppe wird in der Konfiguration der Aktivität gespeichert. Die Aktivität verwendet diesen Kennzeichner, um die Gruppe bei der Berechnung der Gruppenliste zum Ausführungszeitpunkt des Arbeitsablaufs auszuwählen.
   - **Objekt aus Arbeitsablauf-Datenkontext.** Die Gruppe wird von der Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt. Bei der Konfiguration einer Aktivität „Aus Gruppe entfernen" können Sie angeben, welche Gruppe von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll.
   - **Durch Regel-Ausdruck des DN-Wertes identifiziertes Objekt.** Der eindeutige Name (Distinguished Name, DN) der Gruppe wird durch den Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration einer Aktivität „Aus Gruppe entfernen" erstellen.

   Klicken Sie zum Löschen einer Gruppe aus der Liste auf die mit **X** markierte **Löschtaste** rechts neben dem Listeneintrag für diese Gruppe.
8. Lassen Sie Benachrichtigungseinstellungen anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von Benachrichtigungen.
9. Lassen Sie Einstellungen für Fehlerbehebung anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von Fehlerbehebungen.
10. Lassen Sie Optionen „Ausführen als" anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von „Ausführen als"-Optionen.
11. Lassen Sie erweiterte Einstellungen anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren zusätzlicher Einstellungen.

Aktivität „Verschieben"

Beim Konfigurieren einer Verschiebeaktivität können Sie die Regeln für die Auswahl des Objekts angeben, die durch die Aktivität verschoben werden sollen, und den Container, in den das Objekt verschoben werden soll (Zielcontainer). Weitere Optionen sind verfügbar: Benachrichtigung, Fehlerbehebung und Optionen „Ausführen als".

Gehen Sie folgendermaßen vor, um eine Verschiebeaktivität zu konfigurieren:

1. Erweitern Sie in der Konsolenstruktur von Quest One ActiveRoles **Konfiguration | Richtlinien | Arbeitsablauf** und wählen Sie dann den Arbeitsablauf, der die Verschiebeaktivität enthält, die Sie konfigurieren möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.
2. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Aktivität und klicken Sie dann auf **Eigenschaften**.
3. Gehen Sie zur Registerkarte **Aktivitätsziel** im Dialogfeld **Eigenschaften der Aktivität „Verschieben"**.

4. Klicken Sie in das Feld **Die Aktivität führt den Vorgang an diesem Objekt aus**, um das Objekt anzugeben, das die Aktivität verschieben soll. Dieses Objekt wird als Aktivitätsziel bezeichnet. Sie können das Aktivitätsziel mit den folgenden Optionen angeben:
   - **Festes Objekt im Verzeichnis.** Das Aktivitätsziel ist das angegebene Objekt. Sie können das gewünschte Objekt bei der Konfiguration der Verschiebeaktivität in Active Directory auswählen.
   - **Vom Arbeitsablaufparameter erkanntes Objekt.** Das Aktivitätsziel ist das Objekt, welches durch den Wert eines bestimmten Arbeitsablaufsparameters angegeben wurde. Sie können den gewünschten Parameter bei der Konfiguration der Verschiebeaktivität aus der Arbeitsablaufdefinition auswählen.
   - **Objekt aus Arbeitsablauf-Datenkontext.** Das Aktivitätsziel wird von der Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt. Bei der Konfiguration der Verschiebeaktivität können Sie angeben, welches Objekt von der Aktivität bei der Ausführung des Arbeitsablaufs ausgewählt werden soll.
   - **Durch Regel-Ausdruck des DN-Wertes identifiziertes Objekt.** Der eindeutige Name (Distinguished Name, DN) des Aktivitätsziels wird durch den Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration der Verschiebeaktivität erstellen.
5. Gehen Sie zur Registerkarte **Zielcontainer** im Dialogfeld **Eigenschaften der Aktivität „Verschieben"**.
6. Klicken Sie zum Angeben der Organisationseinheit (OE) oder des Containers, in den die Aktivität das Zielobjekt verschieben soll, in das Feld **Die Aktivität verschiebt das Objekt in diesen Container**. Sie können unter den folgenden Optionen wählen:
   - **Fester Container im Verzeichnis.** Bei Auswahl dieser Option verschiebt die Aktivität das Objekt in die jeweilige Organisationseinheit oder den Container. Sie können die gewünschte Organisationseinheit oder den gewünschten Container in Active Directory auswählen, wenn Sie die Aktivität „Verschieben" konfigurieren.
   - **Aktivitätszielobjekt.** Bei Auswahl dieser Option verschiebt die Aktivität das Objekt in die Organisationseinheit oder den Container, die bzw. der von einer anderen CRUD-Aktivität erstellt oder anderweitig bearbeitet wurde. Sie können die gewünschte CRUD-Aktivität aus der Arbeitsablaufdefinition auswählen, wenn Sie die Aktivität „Verschieben" konfigurieren.
   - **Vom Arbeitsablaufparameter erkanntes Objekt.** Bei Auswahl dieser Option verschiebt die Aktivität das Objekt in die Organisationseinheit oder den Container, die bzw. der durch einen bestimmten Wert des Arbeitsablaufparameters festgelegt wurde. Sie können den gewünschten Parameter bei der Konfiguration der Verschiebeaktivität aus der Arbeitsablaufdefinition auswählen.
   - **Objekt aus dem Arbeitsablaufdatenkontext.** Bei Auswahl dieser Option verschiebt die Aktivität das Objekt in die Organisationseinheit oder den Container, die bzw. der von der Aktivität „Verschieben" auf der Grundlage der zum Zeitpunkt der Ausführung des Arbeitsablaufs in der Arbeitsablaufumgebung gefundenen Daten ausgewählt wurde. Bei der Konfiguration einer Verschiebungsaktivität können Sie angeben, welche Organisationseinheit bzw. welcher Container von der Aktivität zum Ausführungszeitpunkt des Arbeitsablaufs ausgewählt werden soll.
   - **Objekt durch Regel-Ausdruck des DN-Werts identifiziert.** Bei Auswahl dieser Option verschiebt die Aktivität das Objekt in die Organisationseinheit oder den Container, deren bzw. dessen eindeutiger Name (Distinguished Name, DN) durch den Zeichenfolgenwert eines bestimmten Regelausdrucks festgelegt wurde. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regel-Ausdruck bei der Konfiguration der Verschiebeaktivität erstellen.

7. Lassen Sie Benachrichtigungseinstellungen anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von Benachrichtigungen.
8. Lassen Sie Einstellungen für Fehlerbehebung anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von Fehlerbehebungen.
9. Lassen Sie Optionen „Ausführen als" anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von „Ausführen als"-Optionen.
10. Lassen Sie erweiterte Einstellungen anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren zusätzlicher Einstellungen.

Aktivität „Deprovisionieren"

Eine Aktivität „Deprovisionieren" dient dazu, die ActiveRoles-Deprovisionierungsrichtlinien auf einen bestimmten Benutzer oder eine bestimmte Gruppe anzuwenden. Mit dieser Aktivität führt ActiveRoles alle von den Deprovisionierungsrichtlinien vorgeschriebenen Aufgaben aus und deprovisioniert so den Benutzer oder die Gruppe.

Wenn Sie eine Aktivität „Deprovisionieren" konfigurieren, können Sie die Regeln zur Auswahl des Benutzers oder der Gruppe festlegen, der bzw. die von der Aktivität deprovisioniert werden soll. Weitere Optionen sind verfügbar: Benachrichtigung, Fehlerbehebung und Optionen „Ausführen als".

Gehen Sie folgendermaßen vor, um eine Deprovisionierungsaktivität zu konfigurieren:

1. Erweitern Sie in der Quest One ActiveRoles Konsolenstruktur den Eintrag **Konfiguration | Richtlinien | Arbeitsablauf**, und wählen Sie dann den Arbeitsablauf, der die Aktivität „Deprovisionieren" enthält, die Sie konfigurieren möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.

2. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Aktivität und klicken Sie dann auf **Eigenschaften**.
3. Rufen Sie die Registerkarte **Aktivitätsziel** im Dialogfeld **Eigenschaften der Aktivität „Deprovisionieren"** auf.
4. Klicken Sie in das Feld **Die Aktivität führt den Vorgang an diesem Objekt aus**, um den Benutzer oder die Gruppe festzulegen, der bzw. die von der Aktivität deprovisioniert werden soll. Dieses Objekt wird als Aktivitätsziel bezeichnet. Sie können das Aktivitätsziel mit den folgenden Optionen angeben:
   - **Festes Objekt im Verzeichnis.** Das Aktivitätsziel ist das angegebene Objekt. Sie können das gewünschte Objekt in Active Directory auswählen, wenn Sie die Aktivität „Deprovisionieren" konfigurieren.
   - **Vom Arbeitsablaufparameter erkanntes Objekt.** Das Aktivitätsziel ist das Objekt, welches durch den Wert eines bestimmten Arbeitsablaufsparameters angegeben wurde. Sie können den gewünschten Parameter aus der Arbeitsablaufdefinition auswählen, wenn Sie die Aktivität „Deprovisionieren" konfigurieren.
   - **Objekt aus Arbeitsablauf-Datenkontext.** Das Aktivitätsziel wird von der Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt. Beim Konfigurieren einer Aktivität „Deprovisionieren" können Sie festlegen, welches Objekt von der Aktivität bei Ausführung des Arbeitsablaufs ausgewählt werden soll.
   - **Durch Regel-Ausdruck des DN-Wertes identifiziertes Objekt.** Der eindeutige Name (Distinguished Name, DN) des Aktivitätsziels wird durch den Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regelausdruck erstellen, wenn Sie die Aktivität „Deprovisionieren" konfigurieren.

5. Lassen Sie Benachrichtigungseinstellungen anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von Benachrichtigungen.
6. Lassen Sie Einstellungen für Fehlerbehebung anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von Fehlerbehebungen.
7. Lassen Sie Optionen „Ausführen als" anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von „Ausführen als"-Optionen.
8. Lassen Sie erweiterte Einstellungen anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren zusätzlicher Einstellungen.

Aktivität „Deprovisionierung aufheben"

Eine Aktivität „Deprovisionierung aufheben" dient dazu, einen bestimmten Benutzer oder eine bestimmte Gruppe wiederherzustellen, der bzw. die mit Hilfe von ActiveRoles deprovisioniert wurde. Mit dieser Aktivität macht ActiveRoles die Änderungen rückgängig, die am Benutzer- oder Gruppenobjekt durch die Anwendung der Deprovisionierungsrichtlinien von ActiveRoles vorgenommen wurden. Daher wird das Objekt in den Zustand zurückversetzt, in dem es sich befand, bevor die deprovisionierungsbezogenen Änderungen vorgenommen wurden.

Wenn Sie eine Aktivität „Deprovisionierung aufheben" konfigurieren, können Sie die Regeln zur Auswahl des Benutzers oder der Gruppe festlegen, der bzw. die von der Aktivität wiederhergestellt werden soll. Weitere Optionen sind verfügbar: Benachrichtigung, Fehlerbehebung und Optionen „Ausführen als".

Gehen Sie folgendermaßen vor, um eine Aktivität „Deprovisionierung aufheben" zu konfigurieren:

1. Erweitern Sie in der Quest One ActiveRoles Konsolenstruktur den Eintrag **Konfiguration | Richtlinien | Arbeitsablauf**, und wählen Sie dann den Arbeitsablauf, der die Aktivität „Deprovisionierung aufheben" enthält, die Sie konfigurieren möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.

2. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Aktivität und klicken Sie dann auf **Eigenschaften**.
3. Rufen Sie die Registerkarte **Aktivitätsziel** im Dialogfeld **Eigenschaften der Aktivität „Deprovisionierung aufheben"** auf.
4. Klicken Sie in das Feld **Die Aktivität führt den Vorgang an diesem Objekt aus**, um den Benutzer oder die Gruppe festzulegen, der bzw. die von der Aktivität wiederhergestellt werden soll. Dieses Objekt wird als Aktivitätsziel bezeichnet. Sie können das Aktivitätsziel mit den folgenden Optionen angeben:
   - **Festes Objekt im Verzeichnis.** Das Aktivitätsziel ist das angegebene Objekt. Sie können das gewünschte Objekt in Active Directory auswählen, wenn Sie die Aktivität „Deprovisionierung aufheben" konfigurieren.
   - **Vom Arbeitsablaufparameter erkanntes Objekt.** Das Aktivitätsziel ist das Objekt, welches durch den Wert eines bestimmten Arbeitsablaufsparameters angegeben wurde. Sie können den gewünschten Parameter aus der Arbeitsablaufdefinition auswählen, wenn Sie die Aktivität „Deprovisionierung aufheben" konfigurieren.
   - **Objekt aus Arbeitsablauf-Datenkontext.** Das Aktivitätsziel wird von der Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt. Beim Konfigurieren einer Aktivität „Deprovisionierung aufheben" können Sie festlegen, welches Objekt von der Aktivität bei Ausführung des Arbeitsablaufs ausgewählt werden soll.
   - **Durch Regel-Ausdruck des DN-Wertes identifiziertes Objekt.** Der eindeutige Name (Distinguished Name, DN) des Aktivitätsziels wird durch den Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben. Durch Verwendung eines Regel-Ausdrucks

können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regelausdruck erstellen, wenn Sie die Aktivität „Deprovisionierung aufheben" konfigurieren.

5. Lassen Sie Benachrichtigungseinstellungen anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von Benachrichtigungen.
6. Lassen Sie Einstellungen für Fehlerbehebung anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von Fehlerbehebungen.
7. Lassen Sie Optionen „Ausführen als" anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von „Ausführen als"-Optionen.
8. Lassen Sie erweiterte Einstellungen anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren zusätzlicher Einstellungen.

Aktivität „Löschen"

Wenn Sie eine Aktivität „Löschen" konfigurieren, können Sie die Regeln zur Auswahl des Objektes festlegen, das von der Aktivität in ActiveDirectory gelöscht werden soll. Weitere Optionen sind verfügbar: Benachrichtigung, Fehlerbehebung und Optionen „Ausführen als".

Gehen Sie folgendermaßen vor, um eine Aktivität „Löschen" zu konfigurieren:

1. Erweitern Sie in der Quest One ActiveRoles Konsolenstruktur den Eintrag **Konfiguration | Richtlinien | Arbeitsablauf**, und wählen Sie dann den Arbeitsablauf aus, der die Aktivität „Löschen" enthält, die Sie konfigurieren möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.

2. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Aktivität und klicken Sie dann auf **Eigenschaften**.
3. Rufen Sie die Registerkarte **Aktivitätsziel** im Dialogfeld **Eigenschaften der Aktivität „Löschen"** auf.
4. Klicken Sie in das Feld **Die Aktivität führt den Vorgang an diesem Objekt aus**, um das Objekt festzulegen, das von der Aktivität gelöscht werden soll. Dieses Objekt wird als Aktivitätsziel bezeichnet. Sie können das Aktivitätsziel mit den folgenden Optionen angeben:
   - **Festes Objekt im Verzeichnis.** Das Aktivitätsziel ist das angegebene Objekt. Sie können das gewünschte Objekt in Active Directory auswählen, wenn Sie die Aktivität „Löschen" konfigurieren.
   - **Vom Arbeitsablaufparameter erkanntes Objekt.** Das Aktivitätsziel ist das Objekt, welches durch den Wert eines bestimmten Arbeitsablaufsparameters angegeben wurde. Sie können den gewünschten Parameter aus der Arbeitsablaufdefinition auswählen, wenn Sie die Aktivität „Löschen" konfigurieren.
   - **Objekt aus Arbeitsablauf-Datenkontext.** Das Aktivitätsziel wird von der Suchaktivität auf Basis der zum Zeitpunkt der Ausführung in der Arbeitsablaufumgebung gefundenen Daten ausgewählt. Wenn Sie eine Aktivität „Löschen" konfigurieren, können Sie festlegen, welches Objekt von der Aktivität bei Ausführung des Arbeitsablaufs ausgewählt werden soll.
   - **Durch Regel-Ausdruck des DN-Wertes identifiziertes Objekt.** Der eindeutige Name (Distinguished Name, DN) des Aktivitätsziels wird durch den Zeichenfolgewert eines bestimmten Regel-Ausdrucks angegeben. Durch Verwendung eines Regel-Ausdrucks können Sie einen Zeichenfolgewert basierend auf den Eigenschaften verschiedener Objekte erstellen, die zum Ausführungszeitpunkt in der Arbeitsablaufumgebung gefunden werden. Sie können den gewünschten Regelausdruck erstellen, wenn Sie die Aktivität „Löschen" konfigurieren.
5. Lassen Sie Benachrichtigungseinstellungen anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von Benachrichtigungen.

6. Lassen Sie Einstellungen für Fehlerbehebung anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von Fehlerbehebungen.
7. Lassen Sie Optionen „Ausführen als" anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren von „Ausführen als"-Optionen.
8. Lassen Sie erweiterte Einstellungen anzeigen oder ändern Sie sie. Anweisungen finden Sie unter Konfigurieren zusätzlicher Einstellungen.

Konfigurieren von Benachrichtigungen

Sie können eine CRUD-Aktivität darauf konfigurieren, Empfänger als Abonnenten der Benachrichtigungen folgender Ereignisse festzulegen:

- **Aktivität erfolgreich abgeschlossen.** Wenn diese Aktivität so konfiguriert wurde, dass Benachrichtigungen über dieses Ereignis erfolgen, versendet ActiveRoles eine Benachrichtigungs-E-Mail, wenn während der Ausführung dieser Aktivität keine erheblichen Fehler festgestellt wurden.
- **Aktivität hat einen Fehler festgestellt.** Wenn diese Aktivität so konfiguriert wurde, dass Benachrichtigungen über dieses Ereignis erfolgen, versendet ActiveRoles eine Benachrichtigungs-E-Mail, wenn während der Ausführung dieser Aktivität erhebliche Fehler festgestellt wurden.

Gehen Sie folgendermaßen vor, um Benachrichtigungen für eine CRUD-Aktivität zu konfigurieren:

1. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Aktivität und klicken Sie dann auf **Eigenschaften**.
2. Rufen Sie die Registerkarte **Benachrichtigung** im Dialogfeld **Eigenschaften** auf, und führen Sie dann das Verfahren zum Konfigurieren einer Benachrichtigungsaktivität aus, um die Benachrichtigungseinstellungen zu konfigurieren.

Die Benachrichtigungseinstellungen geben das Ereignis an, über das eine Benachrichtigung versendet werden soll, sowie die Empfänger der Benachrichtigung. Wenn sie vom Arbeitsablauf ausgeführt wird, verfasst diese Aktivität eine dem angegebenen Ereignis entsprechende Benachrichtigung. ActiveRoles hält die von der Aktivität vorbereitete Meldung zurück und sendet die Meldung bei Eintritt des Ereignisses an die angegebenen Empfänger.

Konfigurieren von Fehlerbehebungen

Wenn Sie eine CRUD-Aktivität konfigurieren, können Sie die Fehlerbehebung konfigurieren, um Fehler zu beseitigen, die von dieser Suchaktivität sowie allen in dieser Aktivität enthaltenen Aktivitäten festgestellt wurden.

Gehen Sie folgendermaßen vor, um die Fehlerbehebung für eine CRUD-Aktivität zu konfigurieren:

1. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Aktivität und klicken Sie dann auf **Eigenschaften**.
2. Rufen Sie die Registerkarte **Fehlerbehebung** im Dialogfeld **Eigenschaften** auf, und aktivieren oder deaktivieren Sie die Option **„Arbeitsablauf fortsetzen" auch dann, wenn bei dieser Aktivität ein Fehlerkontrollkästchen** auf dieser Registerkarte festgestellt wurde.

Wenn **Arbeitsablauf fortsetzen, auch wenn bei dieser Aktivität ein Fehler festgestellt wird** markiert ist (Standardeinstellung), beendet ActiveRoles bei einem bei dieser Aktivität festgestellten Fehler den Arbeitsablauf. Wenn Sie dieses Kontrollkästchen markieren, wird der Arbeitsablauf unabhängig davon, ob bei der Aktivität ein Fehler erkannt wird, fortgesetzt.

Konfigurieren von „Ausführen als"-Optionen

Standardmäßig werden CRUD-Aktivitäten unter dem Benutzerkonto ausgeführt, das in der „Ausführen als"-Einstellung in den Arbeitsablaufoptionen und den Startbedingungen festgelegt wurde. Dabei kann es sich um das Dienstkonto des ActiveRoles-Verwaltungsdienstes oder um das Konto des Benutzers handeln, der den Start des Arbeitsablaufs ausgelöst hat. Sie können die Aktivität so konfigurieren, dass sie die Standardeinstellung für „Ausführen als" ersetzt.

Gehen Sie folgendermaßen vor, um „Ausführen als"-Optionen für eine CRUD-Aktivität zu konfigurieren:

1. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Aktivität und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie auf die Verknüpfung **„Ausführen als"-Optionen** unten im Dialogfeld **Eigenschaften**.
3. Markieren Sie zum Ersetzen der Standardeinstellung „Ausführen als" für diese Aktivität das Kontrollkästchen **Diese Aktivität ausführen unter** und wählen Sie das Konto, unter dem diese Aktivität ausgeführt werden soll:
   - Klicken Sie auf **Das Dienstkonto von Quest One ActiveRoles**, wenn dieser Aktivität unter dem Dienstkonto des ActiveRoles Verwaltungsdiensts ausgeführt werden soll.
   - Klicken Sie auf **Das Konto des Benutzers, der mit dem Arbeitsablauf begonnen hat**, wenn diese Aktivität unter dem Konto des Benutzers ausgeführt werden soll, der den Arbeitsablauf initialisiert hat. In Abhängigkeit vom Arbeitsablauftyp ist dies der Benutzer, der den Vorgang angefragt hat, mit dem der Arbeitsablauf gestartet wurde, oder der Benutzer, der den Arbeitsablauf auf Anfrage gestartet hat.

   Das Konto, unter dem die Aktivität ausgeführt wird, bestimmt die Zugriffsrechte der Aktivität im Verzeichnis.
4. Unter der Überschrift **Genehmigungsdurchsetzungsoption** können Sie die Einstellungen anzeigen oder ändern.

   Mit den Einstellungen für die **Genehmigungsdurchsetzung** legen Sie fest, ob der von der Aktivität angeforderte Vorgang auf die Genehmigungsregeln angewendet werden soll, wenn die Aktivität unter einem berechtigten Konto, wie etwa dem ActiveRoles-Dienstkonto, einem ActiveRoles-Admin-Konto oder dem Konto des Benutzers, der als genehmigende Instanz festgelegt wurde, ausgeführt wird. Die folgenden Einstellungen sind verfügbar:

   - **Von den Arbeitsablaufoptionen und den Startbedingungen erben.** Wählen Sie diese Option, wenn Sie möchten, dass die Aktivität die Genehmigungsdurchsetzungsoption verwendet, die in den Arbeitsablaufoptionen und den Startbedingungen ausgewählt wurde.
   - **Folgende Option für diese Aktivität verwenden.** Klicken Sie auf diese Option, und aktivieren oder deaktivieren Sie dann das Kontrollkästchen **Genehmigung erzwingen**, wenn Sie möchten, dass diese Aktivität die Genehmigungsdurchsetzungsoption aufhebt, die in den Arbeitsablaufoptionen und den Startbedingungen ausgewählt wurde.

   Durch Aktivieren des Kontrollkästchens **Genehmigung erzwingen** wird die Genehmigungsregel angewendet, und der Vorgang wird unabhängig vom Konto, unter dem die Aktivität ausgeführt wird, zur Genehmigung eingereicht. Ansonsten umgeht der von der Aktivität angeforderte Vorgang die Genehmigungsregeln, wenn die Aktivität unter dem ActiveRoles-Dienstkonto, einem ActiveRoles-Administratorkonto oder unter dem Konto des Benutzers ausgeführt wird, der als Genehmiger bestimmt wurde. Somit wird der Vorgang nicht zur Genehmigung eingereicht.

Konfigurieren zusätzlicher Einstellungen

Mit Hilfe der zusätzlichen Einstellungen können Sie den standardmäßigen Text „Grund für den Vorgang" überschreiben und sogenannte „Anforderungskontrollen" hinzufügen, um das Verhalten der Aktivität zu ändern.

Gehen Sie folgendermaßen vor, um zusätzliche Einstellungen für eine CRUD-Aktivität zu konfigurieren:

1. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Aktivität und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie auf die Verknüpfung **Zusätzliche Einstellungen** unten im Dialogfeld **Eigenschaften**.
3. Im Dialogfeld **Zusätzliche Einstellungen** können Sie die folgenden Optionen anzeigen oder ändern:
   - **Diesen Text anstelle des ursprünglichen Texts für die Vorgangsbegründung verwenden.** Wenn der von der CRUD-Aktivität angeforderte Vorgang zur Genehmigung eingereicht werden muss, können Sie den Begründungstext für den Vorgang angeben, der dem Genehmiger anstatt jenes Begründungstextes angezeigt wird, welcher in der Vorgangsanforderung angegeben wurde, die den Arbeitsablauf gestartet hat.

     Aktivieren Sie das Kontrollkästchen **Diesen Text anstelle des ursprünglichen Textes „Grund für den Vorgang" verwenden**, und geben Sie den entsprechenden Text „Grund für den Vorgang" ein, der anstelle des ursprünglichen Textes „Grund für den Vorgang" verwendet werden soll. Aktivieren Sie das Kontrollkästchen **Nur dann verwenden, wenn der Grund für den Vorgang ursprünglich nicht angegeben wurde**, wenn Sie möchten, dass die Aktivität Ihren Text „Grund für den Vorgang" nur dann verwendet, wenn bei der Vorgangsanforderung, die den Arbeitsablauf ausgelöst hat, kein Text „Grund für den Vorgang" festgelegt wurde.
   - **Zulassen, dass die durch diese Aktivität erstellte Anforderung eine neue Instanz des Arbeitsablaufs, die diese Aktivität enthält, startet.** Dieses Kontrollkästchen sollte normalerweise deaktiviert werden, um zu verhindern, dass die Aktivität in der Situation, bei welcher der Vorgang, der von dieser Aktivität innerhalb eines bestimmten Arbeitsablaufs angefordert wird, die Startbedingungen dieses Arbeitsablaufs erfüllt. Das Aktivieren dieses Kontrollkästchens könnte zu einer Schleife führen, in welcher die Arbeitsablaufinstanzen immer wieder die gleiche Aktivität ausführen, was letztendlich einen Speicherüberlauf verursachen könnte.
   - **Anforderungskontrollen in die Aktivitäts-Vorgangsanforderung aufnehmen oder ausschließen.** Anforderungskontrollen sind bestimmte Datenelemente in einer Vorgangsanforderungen, die verwendet werden können, um ActiveRoles zusätzliche Informationen darüber zur Verfügung zu stellen, wie die Anforderung verarbeitet werden soll. Anforderungskontrollen sind optional. Informationen über Anforderungskontrollen finden Sie in Active Roles SDK.

     Klicken Sie zum Hinzufügen oder Änderungen einer Kontrolle auf **Hinzufügen** bzw. **Ändern** und geben Sie im daraufhin angezeigten Dialogfeld den Namen und, sofern vorhanden, den Wert der Kontrolle ein. Wenn die Aktivität die Kontrolle zu den Anforderungen hinzufügen soll, klicken Sie auf **Diese Kontrolle in die Aktivitäts-Vorgangsanforderungen aufnehmen**. Wenn Sie sichergehen möchten, dass die Kontrolle nie in den von dieser Aktivität erstellten Anforderungen erscheint, klicken Sie auf **Diese Kontrolle aus den Aktivitäts-Vorgangsanforderungen ausschließen**.

Aktivieren oder Deaktivieren einer Aktivität

Die temporäre Deaktivierung einer Aktivität kann nützlich sein, wenn an dem Arbeitsablauf gearbeitet wird, sodass die Arbeitsablaufdefinition noch nicht abgeschlossen ist und die Aktivität bis zu einem späteren Zeitpunkt nicht ausgeführt werden soll.

Gehen Sie folgendermaßen vor, um eine Aktivität zu deaktivieren bzw. um eine deaktivierte Aktivität zu aktivieren:

1. Wählen Sie die Arbeitsablaufdefinition in der Konsolenstruktur, um den Arbeitsablauf als Prozessdiagramm anzuzeigen.
2. Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf die Aktivität, und klicken Sie dann auf **Deaktivieren** bzw. **Aktivieren**.

Wenn eine Aktivität in einem bestimmten Arbeitsablauf deaktiviert ist, überspringt ActiveRoles diese Aktivität beim Ausführen dieses Arbeitsablaufs. Wenn Sie eine Aktivität in einem bestimmten Arbeitsablauf deaktivieren, ermöglichen Sie, dass ActiveRoles diese Aktivität beim Ausführen des Arbeitsablaufs mit ausführt.

Aktivieren oder Deaktivieren eines Arbeitsablaufs

Die temporäre Deaktivierung eines Arbeitsablaufs kann nützlich sein, wenn an dem Arbeitsablauf gearbeitet wird, sodass die Arbeitsablaufdefinition noch nicht abgeschlossen ist und die im Arbeitsablauf enthaltenen Aktivitäten bis zu einem späteren Zeitpunkt nicht ausgeführt werden sollen.

Gehen Sie folgendermaßen vor, um einen Arbeitsablauf zu deaktivieren bzw. um einen deaktivierten Arbeitsablauf zu aktivieren:

- Klicken Sie mit der rechten Maustaste auf die Arbeitsablaufdefinition in der Konsolenstruktur, und klicken Sie dann auf **Arbeitsablauf deaktivieren** bzw. **Arbeitsablauf aktivieren**.

Wenn ein Arbeitsablauf deaktiviert ist, führt ActiveRoles unabhängig von den Startbedingungen für den Arbeitsablauf keine Aktivitäten aus, die in diesem Arbeitsablauf enthalten sind. Wenn Sie einen deaktivierten Arbeitsablauf aktivieren, erlauben Sie ActiveRoles die Ausführung der in diesem Arbeitsablauf enthaltenen Aktivitäten.

Beispiel: Genehmigungs-Arbeitsablauf

Der Genehmigungs-Arbeitsablauf ergänzt die automatisierten Richtlinien, um Bereitstellungs- und Deprovisionsentscheidungen auf der Grundlage von Eingaben durch den Menschen zu treffen. Während automatisierte Richtlinien keinen manuellen Eingriff erfordern, erweitert die auf Genehmigungen basierende Durchführung administrativer Vorgänge die Prozessautomatisierung um die Möglichkeit, Vorgangsanforderungen manuell zu akzeptieren oder zurückzuweisen und die Ausführung von anforderungsverarbeitenden Aufgaben zu überwachen, um zu gewährleisten, dass diese zeitnah beantwortet werden. Der Genehmigungs-Arbeitsablauf kann für eine Vielzahl von Anforderungen genutzt werden.

Bei diesen Anforderungen handelt es sich um Benutzervorgänge, die zur Durchführung von Verwaltungsvorgängen dienen. Als Beispiel für derartige Vorgänge seien hier nur die Erstellung, Änderung und Deprovisionierung von Benutzerkonten genannt.

Wenn ein angeforderter Vorgang die Berechtigung durch bestimmte Personen in einer Organisation erfordert, kann ein Arbeitsablauf zur Koordination des Genehmigungsprozesses gestartet werden. Das System führt den angeforderten Vorgang erst durch, wenn eine autorisierte Person die entsprechende Genehmigung erteilt hat.

Quest One ActiveRoles Administratoren können Genehmigungs-Arbeitsabläufe mit Hilfe von Workflow Designer – einem grafischen Tool, das in der Quest One ActiveRoles-Konsole für die Erstellung von Arbeitsabläufen bereitgestellt wird – erstellen und konfigurieren. Beim Entwurf eines Genehmigungs-Arbeitsablaufs gibt der Administrator an, welche Art von Vorgang zum Start des Arbeitsablaufs führt, und fügt Genehmigungsregeln zum Arbeitsablauf hinzu. Die Genehmigungsregeln legen fest, wer autorisiert ist, den Vorgang zu genehmigen. Sie legen außerdem die erforderliche Reihenfolge der Genehmigungen und die Personen, die über Genehmigungsaufgaben oder Entscheidung informiert werden sollen, fest.

Der von Quest One ActiveRoles bereitgestellte Genehmigungs-Arbeitsablauf umfasst die folgenden Komponenten:

- Der Workflow Designer für die Erstellung von Arbeitsabläufen, der in der Quest One ActiveRoles-Konsole verfügbar ist. Verwenden Sie den Workflow Designer, um einen Genehmigungs-Arbeitsablauf durch Hinzufügen von Genehmigungsaktivitäten zur Arbeitsablaufdefinition zu konfigurieren.
- Die Verzeichnisverwaltungsschnittstellen wie etwa das Web-Interface oder die Quest One ActiveRoles-Konsole für das Senden von Vorgangsanforderungen zur Genehmigung. Der Genehmigungs-Arbeitsablauf kann beispielsweise so konfiguriert werden, dass die Erstellung eines Benutzerkontos über Quest One ActiveRoles den Genehmigungs-Arbeitsablauf startet, anstatt sofort die Benutzererstellung zu beginnen.
- Der mit der Genehmigung zusammenhängende Bereich des Web-Interface für die Verwaltung von Vorgangsanforderungen. Dieser Bereich enthält eine Aufgabenliste für die Genehmigungsaufgaben, die ein festgelegter Benutzer ausführen muss. Diese Liste ermöglicht es dem Benutzer, Aufgaben wie etwa das Genehmigen oder Zurückweisen von Vorgangsanforderungen auszuführen.

Begriffsdefinition

In diesem Abschnitt sind einige wichtige, für den Genehmigungs-Arbeitsablauf geltende Definitionen zusammengefasst.

Genehmigung

Ein Entscheidungspunkt in einem Arbeitsablauf, der verwendet wird, um vor dem Fortsetzen des Arbeitsablaufs die Genehmigung von einer Person zu erhalten.

Genehmigungsregel (Genehmigungsaktivität)

Arbeitsablaufaktivitäten der Kategorie „Genehmigung" werden als „Genehmigungsregeln" bezeichnet. Die Arbeitsablauf-Startbedingungen geben an, welche Vorgänge den Arbeitsablauf starten. Die zum Arbeitsablauf hinzugefügten Genehmigungsregeln bestimmen, wer den Vorgang genehmigen darf, in welcher Reihenfolge die Genehmigungen erfolgen sollen und wer über Genehmigungsaufgaben oder Entscheidungen benachrichtigt werden soll.

Genehmigungsaufgabe

Eine als Teil der Verarbeitung einer Genehmigungsregel erstellte und einer genehmigenden Instanz zugewiesene Aufgabe. Von der genehmigenden Instanz wird die Erfüllung der Aufgabe erwartet, d.h. sie muss die Entscheidung treffen, ob der Vorgang zulässig ist oder abgelehnt werden soll.

Genehmigende Instanz

Die für die Durchführung einer Genehmigungsaufgabe bestimmte Person. Die Einstellung, die die genehmigenden Instanzen festlegt, ist ein Konfigurationselement einer Genehmigungsregel. Bei der Verarbeitung einer Genehmigungsregel erstellt Quest One ActiveRoles eine Genehmigungsaufgabe und weist sie dann den von der Regel definierten genehmigenden Instanzen zu. Der Status der Aufgabe bestimmt den Übergang des Arbeitsablaufs: die Aufgabe muss die Auflösung „Genehmigen" erhalten, damit der Vorgang der Genehmigungsregel entspricht. Wenn der Aufgabe die Auflösung „Zurückweisen" zugewiesen wird, wurde der Vorgang verweigert, und die Arbeitsablaufinstanz ist abgeschlossen.

Initiator (Anforderer)

Die Identität des Benutzers oder Dienstes, der einen Vorgang in Quest One ActiveRoles angefordert hat. Wenn zum Beispiel die Quest One ActiveRoles-Konsole verwendet wird, um ein Objekt zu ändern oder zu erstellen, wird der Konsolenbenutzer als der Initiator des entsprechenden Vorgangs identifiziert. Der Initiator eines Vorgangs wird auch als „Vorgangsanforderer" bezeichnet.

Benachrichtigung

Die Mittel, die für die Benachrichtigung eines Benutzers oder einer Gruppe von Benutzern über eine bestimmte vordefinierte Situation, die sich innerhalb eines Arbeitsablaufs ergeben, kann verwendet werden. Eine Benachrichtigungsmeldung wird generiert und per E-Mail an die angegebenen Empfänger gesendet, um sie über den Eintritt eines bestimmten Ereignisses wie etwa das Senden einer neuen Genehmigungsaufgabe an die genehmigenden Instanzen oder den Abschluss des Vorgangs zu informieren. Eine Benachrichtigungskonfiguration, gespeichert als Teil einer Genehmigungsregel, umfasst solche Elemente wie etwa das Ereignis, bei dessen Eintritt eine Benachrichtigung erfolgen soll, die Liste der Benachrichtigungsempfänger und die Vorlage für die Benachrichtigungsmeldung. Quest One ActiveRoles bietet zusätzlich zu Genehmigungsregeln noch eine separate Arbeitsablauf-Aktivitätskategorie zum Zwecke der Benachrichtigung.

Vorgang

Eine Anforderung für bestimmte, an Verzeichnisdaten vorzunehmende Änderungen wie etwa die Erstellung von Benutzern oder das Hinzufügen von Benutzern zu Gruppen. Ein Vorgang kann einen Genehmigungs-Arbeitsablauf starten. In diesem Fall werden die angeforderten Änderungen nur durchgeführt, nachdem sie genehmigt wurden.

Zielobjekt des Vorgangs

Das vom Vorgang zu ändernde oder zu erstellende Objekt. Wenn beispielsweise die Erstellung eines Benutzerkontos angefordert wird, wird das Konto als „Zielobjekt des Vorgangs" bezeichnet. Bei einer Anforderung zum Hinzufügen eines Benutzers zu einer Gruppe wird die Gruppe als das „Zielobjekt des Vorgangs" bezeichnet.

Funktionsweise

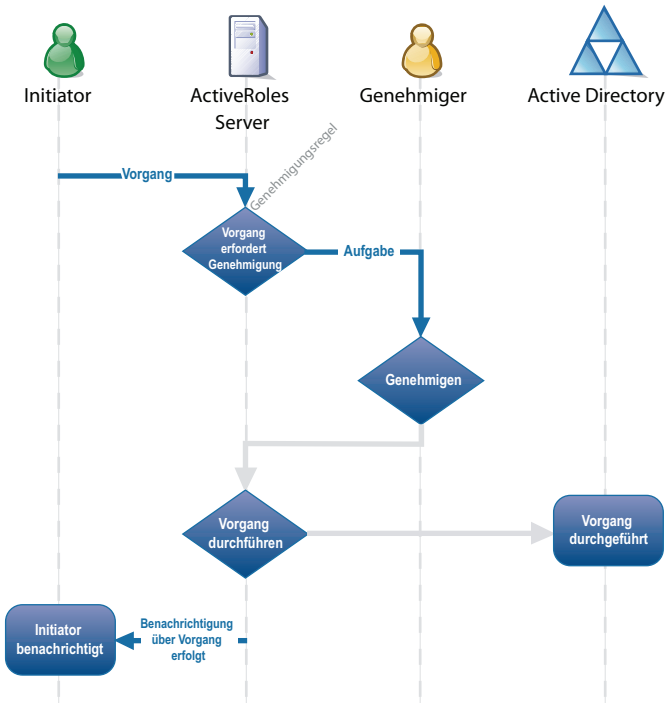
Der Genehmigungs-Arbeitsablauf wird durch Arbeitsablauf-Startbedingungen und Genehmigungsregeln gesteuert. Arbeitsablauf-Startbedingungen legen fest, welche Art von Vorgang den Start des Arbeitsablaufs bewirkt. Die zum Arbeitsablauf hinzugefügten Genehmigungsregeln legen die Personen fest, die autorisiert sind, den Vorgang zu genehmigen (genehmigende Instanzen).

Wenn ein Quest One ActiveRoles-Benutzer einen Vorgang anfordert, führt Quest One ActiveRoles eine Überprüfung durch, um zu ermitteln, ob der Vorgang den Startbedingungen eines Arbeitsablaufs entspricht, und startet dann den Arbeitsablauf, dessen Bedingungen erfüllt sind. Eine im Arbeitsablauf enthaltene Genehmigungsregel generiert dann eine Genehmigungsaufgabe und weist sie den von der Regel definierten genehmigenden Instanzen zu.

Eine genehmigende Instanz schließt eine Genehmigungsaufgabe ab, indem sie die Aktion „Genehmigen" oder „Zurückweisen" auf die Aufgabe anwendet. Hierdurch ändert sich der Status der Aufgabe von „Ausstehend" in „Genehmigt" bzw. „Zurückgewiesen".

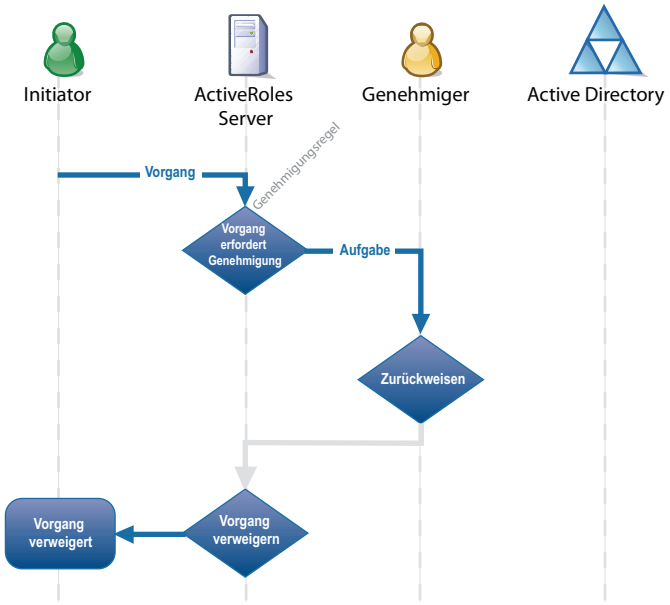
Vorgang: Genehmigen

Wenn die genehmigende Instanz den Vorgang „Genehmigen" auf die Aufgabe anwendet, ermöglicht Quest One ActiveRoles die Durchführung des Vorgangs:



Vorgang: Ablehnen

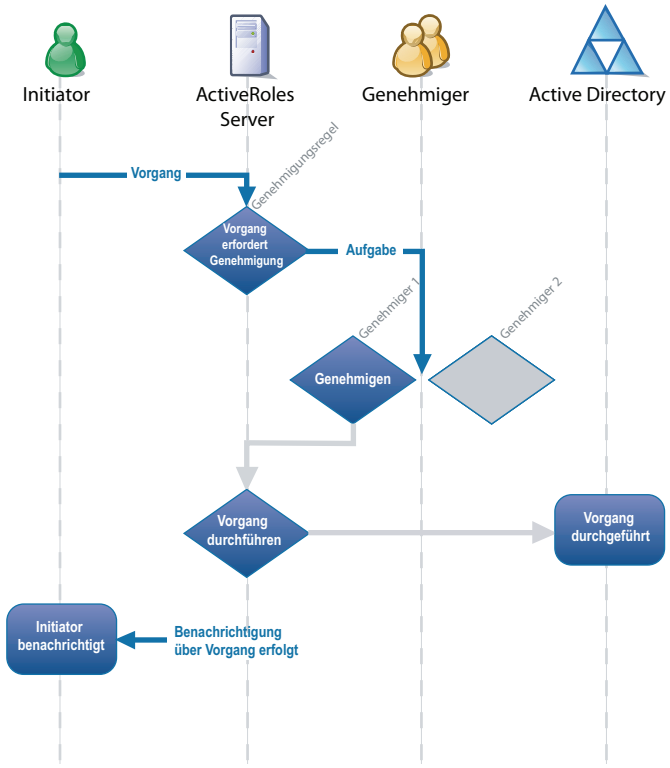
Wenn die genehmigende Instanz den Vorgang „Zurückweisen" auf die Aufgabe anwendet, bricht Quest One ActiveRoles den Vorgang ab:



Mehrere Genehmigungsstellen

Eine Genehmigungsregel kann so konfiguriert werden, dass eine einzelne Aufgabe mehreren Genehmigungsstellen zugeordnet wird. So kann zum Beispiel eine Gruppe als eine genehmigende Instanz bestimmt werden, was dazu führt, dass die Aufgabe jedem Mitglied der Gruppe zugewiesen wird. In diesem Fall schließt der erste der Genehmiger, der den Vorgang „Genehmigen" oder „Zurückweisen" auf die Aufgabe anwendet, die Aufgabe ab.

Wenn der Vorgang „Genehmigen" auf die Aufgabe angewendet wird, ermöglicht Quest One ActiveRoles die Durchführung des Vorgangs. Wenn der Vorgang „Zurückweisen" auf die Aufgabe angewandt wird, bricht Quest One ActiveRoles den Vorgang ab.

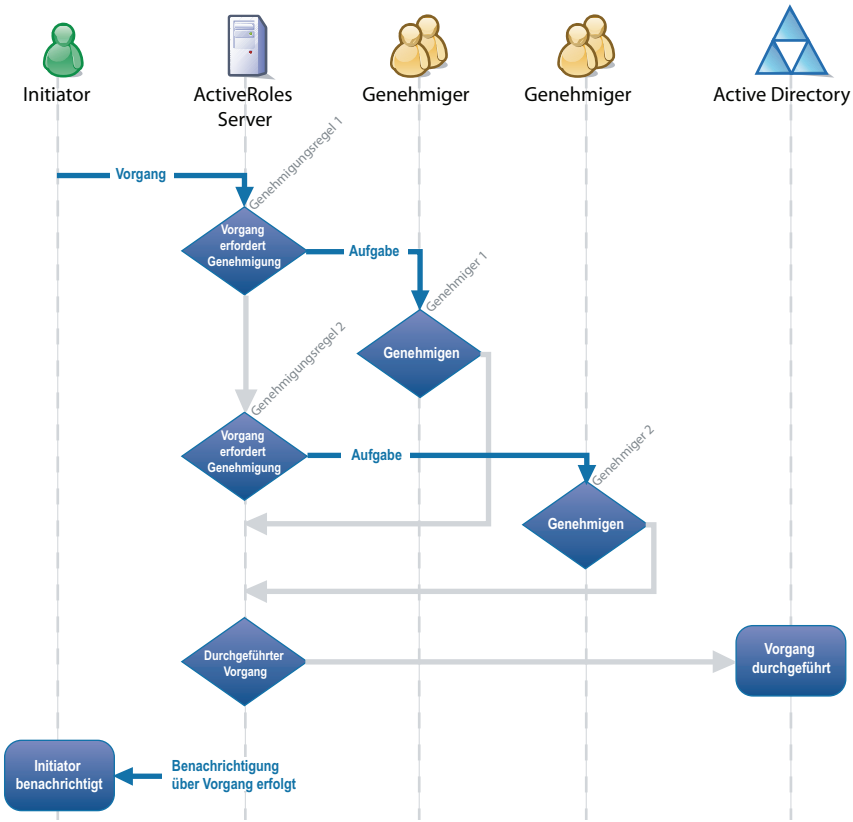


Mehrere Aufgaben

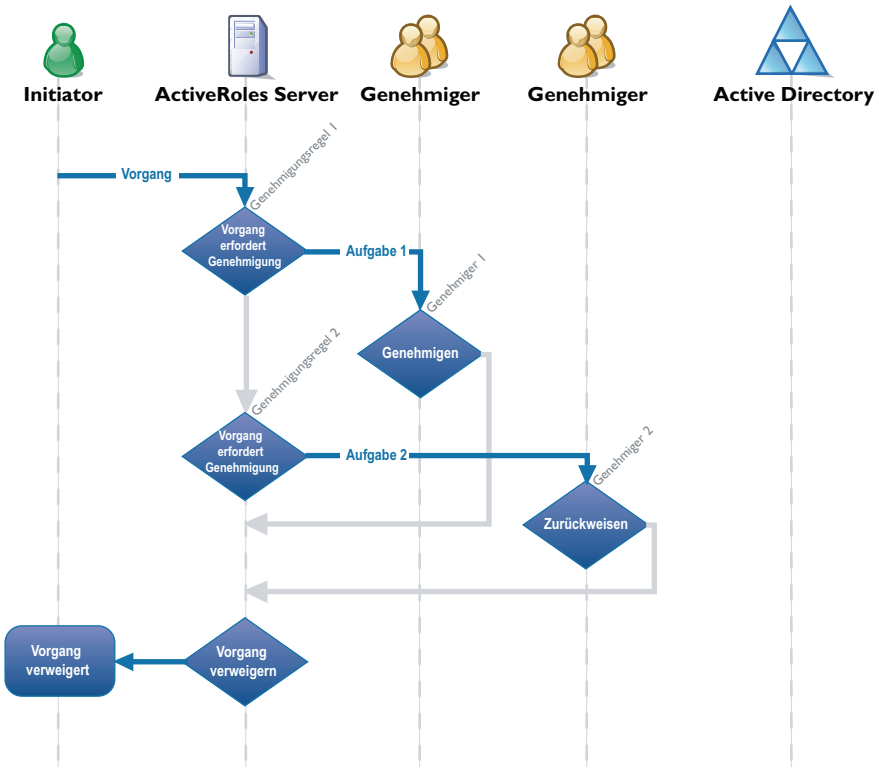
Die Anzahl der von einer einzigen Arbeitsablaufinstanz generierten Genehmigungsaufgaben hängt davon ab, wie viele Genehmigungsregeln im Arbeitsablauf enthalten sind (eine Aufgabe je Regel). Daher werden, wenn ein Arbeitsablauf mehrere Genehmigungsregeln enthält, mehrere Aufgaben erstellt und den entsprechenden genehmigenden Instanzen zugewiesen.

Innerhalb eines einzelnen Arbeitsablaufs werden Genehmigungsregeln nacheinander (sequenziell) angewandt. Das bedeutet, dass eine nachfolgende Regel nur angewandt wird, wenn der angeforderte Vorgang der vorherigen Regel entspricht.

Wenn der Vorgang „Genehmigen" auf alle Aufgabe angewendet wird, ermöglicht Quest One ActiveRoles die Durchführung des Vorgangs.



Wenn auf mindestens eine der Aufgaben der Vorgang „Zurückweisen" angewandt wird, bricht Quest One ActiveRoles den Vorgang ab:



Erstellen und Konfigurieren eines Genehmigungs-Arbeitsablaufs

Um ein Genehmigungsszenario zu implementieren, in dem bestimmte Vorgänge die Genehmigung in Quest One ActiveRoles erfordern, erstellen Sie eine Arbeitsablaufdefinition, konfigurieren dann die Arbeitsablauf-Startbedingungen, fügen Genehmigungsaktivitäten (Genehmigungsregeln) hinzu und konfigurieren diese Ihren Anforderungen entsprechend. Jede dieser Aufgaben wird mit Hilfe von Workflow Designer – einem in der Quest One ActiveRoles-Konsole enthaltenen grafischen Tool – durchgeführt.

Bei der Konfiguration von Arbeitsablauf-Startbedingungen geben Sie Folgendes an:

- Vorgangstyp wie etwa „Erstellen", „Umbenennen", „Ändern" oder „Löschen"; der Arbeitsablauf startet nur dann, wenn ein Vorgang dieses Typs angefordert wird.
- Objekttyp wie etwa „Benutzer", „Gruppe" oder „Computer"; der Arbeitsablauf startet nur dann, wenn der Vorgang Änderungen an einem Objekt dieses Typs anfordert.
- Für den Vorgangstyp „Ändern" eine Liste der Objekteigenschaften; der Arbeitsablauf startet nur dann, wenn der Vorgang Änderungen an irgendeiner dieser Eigenschaften eines Objekts anfordert.
- Identität eines Vorgangsanforderers (Initiator) wie etwa ein Benutzer, eine Gruppe oder ein Dienst; der Arbeitsablauf startet nur dann, wenn der Vorgang im Namen dieser Identität angefordert wird.

- Container wie etwa eine Organisationseinheit oder eine verwaltete Einheit; der Arbeitsablauf startet nur dann, wenn der Vorgang Änderungen an bzw. die Erstellung von einem Objekt in diesem Container anfordert.
- Optional ein Filter, der alle zusätzlichen Bedingungen für die an einem Vorgang beteiligten Einheiten definiert; Der Arbeitsablauf startet nur dann, wenn der Vorgang diesen Bedingungen entspricht. Wenn kein Filter festgelegt ist, dann sind keine zusätzlichen Bedingungen gültig.

Jeder Vorgang, der alle für einen Arbeitsablauf angegebenen Startbedingungen erfüllt, führt zum Start des Arbeitsablaufs.

Bei der Konfiguration einer Genehmigungsregel innerhalb eines Arbeitsablaufs geben Sie Folgendes an:

- Eine Liste der genehmigenden Instanzen wie etwa Benutzer oder Gruppen; diese Einstellung gibt die Personen an, die autorisiert sind, Vorgänge zuzulassen oder zu verweigern, die den Arbeitsablauf starten.
- Benachrichtigungseinstellungen wie etwa Arbeitsablaufereignisse, bei deren Eintreten eine Benachrichtigung erfolgen soll, Benachrichtigungsempfänger, Übermittlungsoptionen und die Benachrichtigungsmeldungsvorlage.

Erstellen einer Arbeitsablaufdefinition

Die Quest One ActiveRoles-Konsole stellt den Workflow-Designer für die Erstellung und Konfiguration der Workflows bereit. Zunächst erstellen Sie eine Arbeitsablaufdefinition. Verwenden Sie dann Workflow Designer, um den Arbeitsablauf zu erstellen, indem Sie Arbeitsablaufaktivitäten hinzufügen und jegliche andere erforderliche Änderungen an der Arbeitsablaufdefinition vornehmen.

Schrittweise Anweisungen finden Sie im Abschnitt Erstellen einer Arbeitsablaufdefinition weiter oben in diesem Kapitel.

Angeben von Arbeitsablauf-Startbedingungen

Sie können die Startbedingungen für einen Arbeitsablauf festlegen, indem Sie seine Definition im Workflow Designer bearbeiten. Die Startbedingungen legen fest, welche Vorgänge zum Start des Arbeitsablaufs führen.

Schrittweise Anweisungen finden Sie im Abschnitt Konfiguration der Workflow-Start-Bedingungen weiter oben in diesem Kapitel.

Beispiel: Angenommen, Sie möchten, dass die Erstellung von Benutzerkonten in einer bestimmten Organisationseinheit eine Genehmigung erfordert. Sie können dieses Szenario implementieren, indem Sie die Arbeitsablauf-Startbedingungen wie folgt konfigurieren:

- Setzen Sie den Vorgangstyp auf „Erstellen".
- Setzen Sie den Objekttyp auf „Benutzer".
- Setzen Sie den Initiator auf „Jeder beliebige Benutzer".
- Legen Sie den Container fest, indem Sie die gewünschte Organisationseinheit auswählen.

Als Ergebnis dieser Bedingungen startet der Arbeitsablauf immer dann, wenn Quest One ActiveRoles für die Erstellung eines Benutzerkontos in dieser Organisationseinheit verwendet wird.

Festlegen der Genehmiger

Bei der Erstellung eines Genehmigungs-Arbeitsablaufs fügen Sie ein oder mehrere Genehmigungsaktivitäten zur Arbeitsablaufdefinition hinzu und erstellen so Genehmigungsregeln. Anschließend konfigurieren Sie Aktivitäten, um die genehmigenden Instanzen für jede Regel zu definieren. Die Organe, die als genehmigende Instanzen festgelegt werden können, umfassen den Vorgesetzten des Vorgangsanforderers, den Verwalter des Zielobjekts des Vorgangs und den Verwalter des Containers, in dem sich das Zielobjekt des Vorgangs befindet. Es ist auch möglich, jeden beliebigen Benutzer oder jede beliebige Benutzergruppe für die Funktion als genehmigende Instanz auszuwählen.

Beispiel. Wir erweitern das vorige Beispiel und nehmen an, dass die Erstellung von Benutzerkonten von dem Verwalter der Organisationseinheit genehmigt werden muss, in der die Konten erstellt werden sollen. Sie können dieses Szenario implementieren, indem Sie eine Genehmigungsaktivität zum Arbeitsablauf hinzufügen und dann den Befehl **Eigenschaften** auf diese Aktivität anwenden, um die entsprechende Option auf der Seite **Genehmigende Instanzen** auszuwählen.

Schrittweise Anweisungen finden Sie im Abschnitt Konfigurieren einer Genehmigungsaktivität weiter oben in diesem Kapitel.

Konfigurieren von Benachrichtigungen

Sie können Genehmigungsregeln konfigurieren, um genehmigende Instanzen oder andere interessierte Parteien über bestimmte Ereignisse zu informieren, die während des Genehmigungsprozesses eintreten können. So kann zum Beispiel eine Genehmigungsregel so konfiguriert werden, dass die durch die Regel festgelegten genehmigenden Instanzen immer dann eine E-Mail-Benachrichtigung erhalten, wenn ein Vorgang angefordert wird, der ihre Genehmigung erfordert. Zu den weiteren Ereignissen, bei deren Eintritt eine Benachrichtigung erfolgen soll, gehört der Abschluss einer Genehmigungsaufgabe. Diese Benachrichtigungen geben an, dass eine genehmigende Instanz die angeforderten Änderungen entweder genehmigt oder verweigert hat. Der Abschluss des Vorgangs gibt an, dass die angeforderten Änderungen angewandt wurden, und das Fehlschlagen eines Vorgangs bedeutet, dass eine Fehlerbedingung vorliegt.

Benachrichtigungsempfänger

Bei der Konfiguration von Benachrichtigungseinstellungen in einer Genehmigungsregel wählen Sie ein Ereignis aus und geben an, wer eine E-Mail-Benachrichtigung bezüglich des Ereignisses erhalten soll (die Benachrichtigungsempfänger). Ein Empfänger kann jeder beliebige Postfach-fähige Benutzer oder jede E-Mail-fähige Gruppe sein. Es gibt auch eine Reihe von Optionen, die es Ihnen ermöglichen, Empfänger auf der Grundlage ihrer Funktion wie etwa einen Vorgangsanforderer, eine genehmigende Instanz, einen Vorgesetzten des Vorgangsanforderers oder einen Verwalter des Zielobjekts des Vorgangs auszuwählen. Es kann eine einzelne Regel konfiguriert werden, um eine Benachrichtigung bezüglich eines oder mehrerer Ereignisse zu senden, wobei eine individuelle Empfängerliste für jedes Ereignis definiert werden kann.

Benachrichtigungsübermittlung

Zusammen mit der Auswahl des Ereignisses, bei dessen Eintritt eine Benachrichtigung erfolgen soll, und der Benachrichtigungsempfänger können Sie auch Übermittlungsoptionen auswählen. Zusätzlich zur sofortigen Übermittlung (was dazu führt, dass bei jedem Eintritt des Ereignisses eine separate Benachrichtigungsmeldung generiert wird) gibt es auch die Möglichkeit der geplanten Übermittlung zur Zusammenfassung mehrerer Benachrichtigungen. Wenn Sie sich für eine geplante Übermittlung entschließen, werden alle Benachrichtigungen über den Eintritt des Ereignisses innerhalb eines frei wählbaren Zeitraums gesammelt und als eine einzige Nachricht gesendet. In diesem Fall besteht der Nachrichtentext aus den zusammengefassten Benachrichtigungen über jedes einzelne Eintreten des Ereignisses.

Benachrichtigungsmeldungen werden zur Übermittlung durch einen SMTP-Dienst wie etwa den von Microsoft Exchange oder Internet Information Services bereitgestellten Dienst weitergeleitet. Die Adresse und weitere Parameter des E-Mail-Servers für ausgehende E-Mails werden im Rahmen der Konfiguration der Benachrichtigungseinstellungen für jede Genehmigungsregel angegeben.

Vorlage für Benachrichtigungsmeldungen

Benachrichtigungsmeldungen basieren auf einer Nachrichtenvorlage, die das Format und den Inhalt von E-Mail-Benachrichtigungen einschließlich des Nachrichtenbetreffs und Nachrichtentexts festlegt. Sie können die Vorlage auf der Seite, auf der Sie ein Ereignis zusammen mit den Benachrichtigungsempfängern auswählen, aufrufen. Wenn Sie die Vorlage ändern, werden die von Ihnen durchgeführten Änderungen nur für die Nachrichten berücksichtigt, die in Zusammenhang mit der von Ihnen konfigurierten Benachrichtigung stehen.

Nachrichtenvorlagen verwenden so genannte Token, um dynamische Inhalte zu Benachrichtigungsmeldungen hinzuzufügen. Sie können Token aus einer Liste auswählen und sie dann zur Nachrichtenvorlage hinzufügen. Jeder Token führt dazu, dass der Nachrichtentext eine bestimmte Information anstelle des Tokens enthält. Wenn Sie eine Nachricht generieren, erfasst das System von den Token repräsentierte Informationen und fügt diese Informationen dann in die Nachricht ein.

Beispiel. Im vorigen Beispiel können Sie die Genehmigungsaktivität so konfigurieren, dass die genehmigende Instanz immer dann eine E-Mail-Benachrichtigung empfängt, wenn die Erstellung eines Benutzers angefordert wird, die eine Genehmigung erfordert. Öffnen Sie die Seite **Eigenschaften** für diese Aktivität und fahren Sie mit dem Schritt **Benachrichtigung** fort. Klicken Sie dann auf **Hinzufügen**, überprüfen Sie, ob das Ereignis **Aufgabe erstellt** markiert ist, und aktivieren Sie das entsprechende Kontrollkästchen unter **Benachrichtigungsempfänger**.

Schrittweise Anweisungen finden Sie im Abschnitt Konfigurieren einer Benachrichtigungsaktivität weiter oben in diesem Kapitel.

E-Mail-basierte Genehmigung

Zusätzlich zu den Web-Interface-Seiten für die Durchführung von Genehmigungsaufgaben bietet Quest One ActiveRoles die Möglichkeit, eine ausstehende Anforderung durch Beantwortung einer Benachrichtigungsmeldung, die über die entsprechende Anforderung informiert, zu genehmigen oder zurückzuweisen. Ein Genehmigungs-Arbeitsablauf kann so konfiguriert werden, das er sich wie folgt verhält:

- Bei Erhalt einer Änderungsanforderung, die eine Genehmigung erfordert, sendet Quest One ActiveRoles eine Benachrichtigungsmeldung an die festlegten genehmigenden Instanzen, wobei der Nachrichtentext die Option zum Genehmigen oder Zurückweisen der Anforderung enthält.
- Die genehmigende Instanz antwortet auf die Benachrichtigungsmeldung und wählt die gewünschte Option—Genehmigen oder Zurückweisen. In der Antwortnachricht muss die genehmigende Instanz einen Kommentar abgeben, der den Grund für die Entscheidung erläutert.
- Quest One ActiveRoles empfängt die Antwortnachricht von der genehmigenden Instanz, überprüft dann, ob die genehmigende Instanz die Anforderung genehmigt oder zurückgewiesen hat, und lässt dann die angeforderten Änderungen zu bzw. weist sie zurück.

Auf diese Weise ist die Möglichkeit, mit Genehmigungsanforderung zu arbeiten, in den E-Mail-Client integriert. Die genehmigenden Instanzen erfordern keinen Webbrowser zum Anzeigen und Beantworten ihrer Genehmigungsanforderungen. Dies ermöglicht zum Beispiel den Anwendern von Microsoft Office Outlook, Genehmigungen selbst dann zu verwalten, wenn sie offline sind. Eine weitere Möglichkeit ist die Verwaltung von Genehmigungen mit Hilfe eines E-Mail-Clients auf einem mobilen Gerät.

Um Genehmigungsanforderungen durch Beantwortung von Benachrichtigungs-E-Mails zu verwalten, müssen Sie als der Besitzer des Postfachs oder als eine Identität, die Vollzugriff (einschließlich der Berechtigung „Senden als") auf das Postfach hat, angemeldet sein. Die Berechtigung „Senden im Namen von" ist nicht ausreichend. Quest One ActiveRoles erkennt eine Situation, in der die Antwort im Namen des Postfachbesitzers gesendet wird, und ignoriert in diesem Fall die Antwortnachricht.

Integration in Microsoft Outlook

Für Organisationen, in denen Microsoft Exchange Server 2007 oder 2010 bereitgestellt wurde, und die Microsoft Office Outlook 2007 oder 2010 als Standard-E-Mail-Client verwenden, bietet Quest One ActiveRoles eine in Outlook integrierte Genehmigungungsverwaltungsfunktion. Dies ermöglicht Microsoft Office-Endbenutzern die Verwaltung von Genehmigungen in Quest One ActiveRoles mit Hilfe der ihnen vertrauten E-Mail-Anwendung.

Die Komponente „Add-in for Outlook", die im Lieferumfang von Quest One ActiveRoles enthalten ist, bietet grundlegende Funktionen für die Verarbeitung und das Senden von Genehmigungen. Quest One ActiveRoles „Add-in for Outlook" ermöglicht Microsoft Outlook-Benutzern, an sie zur Genehmigung gesendete Anforderungen zu genehmigen oder zurückzuweisen. Anforderungen werden über Benachrichtigungs-E-Mails gesendet und können direkt und ohne Verwendung der Web-Interface-Seiten von Quest One ActiveRoles ausgehend von der Benachrichtigungs-E-Mail genehmigt bzw. zurückgewiesen werden. Quest One ActiveRoles Add-in for Outlook fügt zu jeder E-Mail-Nachricht von Quest One ActiveRoles, die über eine Genehmigungsanforderung informiert, die Schaltflächen **Genehmigen** und **Zurückweisen** sowie die Menübefehle **Genehmigen** und **Zurückweisen** hinzu, die es der genehmigenden Instanz ermöglichen, durch Auswahl der entsprechenden Schaltfläche oder des entsprechenden Befehls auf die Anforderung zu antworten.

Software- und Konfigurationsvoraussetzungen

Für die Integration in Microsoft Office Outlook werden die folgende Software und Konfiguration vorausgesetzt:

- **Microsoft Exchange Server 2007 oder 2010.** Die Integration in Outlook erfordert, das in Ihrer Exchange-Organisation mindestens ein Server installiert ist, der die Client Access-Serverfunktion und die Funktion eines Postfachservers übernimmt und Exchange 2007 oder 2010 ausführt.
- **Microsoft Office Outlook 2007 oder 2010.** Die genehmigenden Instanzen verwenden Outlook 2007 oder 2010 als ihre E-Mail-Client-Anwendung.
- **Quest One ActiveRoles Add-in for Outlook.** Die Komponente „Add-in for Outlook" von Quest One ActiveRoles ist auf dem Computer installiert, der Microsoft Office Outlook ausführt. Die spezifischen Softwarevoraussetzungen für Quest One ActiveRoles Add-in for Outlook sind in den Quest One ActiveRoles Versionshinweisen aufgeführt.
- **Postfächer der genehmigenden Instanzen.** Die Postfächer, in denen die Genehmigung und Zurückweisung erfolgt, befinden sich auf einem Postfachserver, auf dem Exchange 2007 oder 2010 ausgeführt wird. Obwohl diese Bedingung nicht obligatorisch ist, wird die Einhaltung dringend empfohlen.
- **Quest One ActiveRoles' Postfach.** Ein ausschließlich für Quest One ActiveRoles reserviertes Postfach. Dieses Postfach sollte sich auf einem Postfachserver befinden, auf dem Exchange 2007 oder 2010 ausgeführt wird.
- **Exchange Web Services.** Für den Genehmigungs-Arbeitsablauf sind die Genehmigungsregel-Benachrichtigungseinstellungen so konfiguriert, dass Quest One ActiveRoles Exchange Web Services für die Kommunikation mit Exchange verwendet. Diese Einstellungen umfassen die Adresse (URL) des Exchange Web Services-Endpunktes auf einem Exchange 2007- oder 2010-Server, der die Client Access-Serverfunktion ausführt und über die Anmeldeinformationen verfügt, die das Postfach von Quest One ActiveRoles identifizieren.

Integration in andere E-Mail-Clients als Outlook

Für Organisationen, die Microsoft Exchange Server 2007 oder 2010 bereitgestellt haben, jedoch eine andere E-Mail-Client-Anwendung als Outlook 2007 oder 2010 verwenden, bietet Quest One ActiveRoles die Möglichkeit, Änderungsanforderungen durch einfache Beantwortung von Benachrichtigungsmeldungen, die die genehmigenden Instanzen über Genehmigungsaufgaben informieren, anzunehmen oder zurückzuweisen. In diesem Fall enthält die Benachrichtigungsmeldung wählbare Optionen. Beim Anklicken dieser Optionen erstellt die E-Mail-Anwendung eine neue Nachricht als Antwort auf die Benachrichtigungsmeldung. Die Antwortnachricht enthält eine Angabe zur Genehmigungsentscheidung (Genehmigt oder Zurückgewiesen) und fordert die genehmigende Instanz auf, einen Kommentar zur Genehmigungsentscheidung zu liefern (Grund für die Genehmigung oder Zurückweisung). Dann sendet die genehmigende Instanz die Antwortnachricht und schließt somit die Genehmigungsaufgabe ab.

Software- und Konfigurationsvoraussetzungen

Die Möglichkeit, Genehmigungen ausgehend von anderen E-Mail-Clients als Outlook zu verwalten, erfordert dieselben Software- und Konfigurationsvoraussetzungen wie die Integration in Outlook (siehe Integration in Microsoft Outlook); es gelten jedoch folgende Ausnahmen und Ergänzugen:

- Die E-Mail-Client-Anwendungen, die für die Verwaltung von Genehmigungen verwendet werden können, sind nicht auf Microsoft Office Outlook 2007 oder 2010 beschränkt. So können zum Beispiel ältere Outlook-Versionen oder E-Mail-Anwendungen auf mobilen Geräten verwendet werden.
- Quest One ActiveRoles Add-in for Outlook muss nicht auf dem Computer installiert sein, auf dem die E-Mail-Client-Anwendung ausgeführt wird.
- Die Genehmigungsregel-Benachrichtigungseinstellungen sind so konfiguriert, dass die von Quest One ActiveRoles erstellten Benachrichtigungsmeldungen auch integriert werden, wenn das Web-Interface ausgeschaltet ist. Stellen Sie sicher, dass die Option **Senden einer Genehmigungsantwort per E-Mail** in den Eigenschaften der E-Mail-Konfiguration, die von der Genehmigungsregel verwendet wird, aktiviert ist (dies ist die Standardeinstellung).

E-Mail-Übertragung über Exchange Web Services

Quest One ActiveRoles kann Exchange Web Services (anstelle des SMTP-Servers) für die Kommunikation mit Exchange Server verwenden, um Benachrichtigungsmeldungen zu senden und eine Antwort auf Benachrichtigungsmeldungen zu erhalten. Dies ermöglicht den Benachrichtigungsempfängern die Durchführung von Genehmigungsaufgaben, indem Sie ausgehend von ihren normalen E-Mail-Clients auf Benachrichtigungsmeldungen antworten, anstatt die Web-Interface-Seiten für die Genehmigung oder Zurückweisung der Anforderungen zu verwenden. Durch die Verwendung von Exchange Web Services ermöglicht Quest One ActiveRoles einem Genehmigungs-Arbeitsablauf das folgende Verhalten:

- Eine Änderungsanforderung, die eine Genehmigung erfordert, führt dazu, dass Quest One ActiveRoles eine Benachrichtigungsmeldung an die festlegte genehmigende Instanz sendet, wobei der Nachrichtentext die Option zum Genehmigen oder Zurückweisen der Anforderung enthält.
- Die genehmigende Instanz antwortet auf die Benachrichtigungsmeldung, indem sie die gewünschte Option (entweder Genehmigen oder Zurückweisen) auswählt und einen Text zur Erläuterung des Entscheidungsgrunds eingibt.
- Quest One ActiveRoles empfängt die Antwortnachricht von der genehmigenden Instanz, überprüft dann, ob die genehmigende Instanz die Anforderung genehmigt oder zurückgewiesen hat, und lässt dann die angeforderten Änderungen zu bzw. weist sie zurück.

Die Verwendung von Exchange Web Services erfordert die Erfüllung der folgenden Voraussetzungen:

- Exchange 2007 oder 2010 in Ihrer Exchange-Organisation. Exchange Web Services ist mit der Funktion „Client-Zugriffsserver" implementiert.
- Spezielles Postfach auf einem Exchange 2007- oder 2010-Server. Das Postfach sollte für die exklusive Verwendung durch Quest One ActiveRoles reserviert sein.

Konfigurationseinstellungen

Die folgenden Konfigurationseinstellungen sind mit der Exchange Web Services-Option für die E-Mail-Übertragung verfügbar:

Exchange Web Services-Adresse

Diese Einstellung legt die URL des Exchange Web Services-Endpunktes fest, der die Datei „exchange.asmx" auf dem Exchange Server angibt, auf dem die Client-Zugriffsserverfunktion ausgeführt wird. Beispiel: https://CAServer.domain.com/EWS/exchange.asmx

Quest One ActiveRoles' Postfach-Anmeldeinformationen

Diese Einstellung gibt den Benutzernamen und das Kennwort des Postfachs an, über das Quest One ActiveRoles E-Mails sendet und empfängt. Das Postfach sollte sich auf einem Exchange 2007- oder Exchange 2010-basierten Postfachserver befinden und für die exklusive Verwendung durch Quest One ActiveRoles reserviert sein.

Es ist wichtig, dass keine anderen Anwendungen als Quest One ActiveRoles auf dieses Postfach zugreifen. Die Verarbeitung von E-Mail-Nachrichten im Postfach von Quest One ActiveRoles durch andere Anwendungen wie etwa Office Outlook kann zu einer Beeinträchtigung der Funktionsweise von Quest One ActiveRoles führen.

Optionen für die Genehmigungs- und Zurückweisungsverknüpfungen

Diese Einstellung kontrolliert das Verhalten der Genehmigungs- und Zurückweisungsverknüpfungen in den Benachrichtigungsmeldungen, die mit Hilfe dieser E-Mail-Konfiguration versandt werden. Es sind zwei Optionen verfügbar:

- **Senden einer Genehmigungsantwort per E-Mail**
- **Genehmigen oder Ablehnen per Web-Interface**

Wenn **Senden einer Genehmigungsantwort per E-Mail** ausgewählt ist, können die Benachrichtigungsempfänger Genehmigungsaufgaben ausgehend von ihrer eigenen E-Mail-Anwendung durchführen. Wenn eine genehmigende Instanz eine der in einer Benachrichtigungsmeldung bereitgestellten Verknüpfungen zum Genehmigen oder Zurückweisen einer Anforderung wählt, antwortet die E-Mail-Anwendung mit einer E-Mail-Nachricht, die Informationen über die Genehmigungsentscheidung enthält. Quest One ActiveRoles empfängt die Antwortnachricht, überprüft dann, ob die genehmigende Instanz die Anforderung genehmigt oder zurückgewiesen hat, und lässt dann die angeforderten Änderungen zu bzw. weist sie zurück.

Wenn **Genehmigen oder Ablehnen per Web-Interface** ausgewählt ist, wird bei Auswahl der Genehmigungs- oder Zurückweisungsverknüpfung in einer Benachrichtigungsmeldung die E-Mail-Anwendung zum Öffnen einer Web-Interface-Seite für die Durchführung der Genehmigungsaufgabe angewiesen. Die Seite wird möglicherweise nicht wie erwartet geöffnet, wenn die E-Mail-Anwendung das HTML-Format nicht unterstützt oder kein entsprechender Webbrowser auf dem Gerät vorhanden ist, auf dem die E-Mail-Anwendung ausgeführt wird.

Verfahren zur Konfiguration der Verwendung von Exchange Web Services

Führen Sie die folgenden Schritte in der Quest One ActiveRoles-Konsole durch, um die Standard-E-Mail-Einstellungen mit der Option zur Verwendung von Exchange Web Services zu konfigurieren:

1. Wählen Sie in der Konsolenstruktur **Konfiguration | Serverkonfiguration | E-Mail-Konfiguration**.
2. Doppelklicken Sie im Bereich „Details" auf **Standard-E-Mail-Einstellungen**.
3. Konfigurieren Sie im Dialogfeld **Standardmäßige Eigenschaften der E-Mail-Einstellungen** die Einstellungen auf der Registerkarte **E-Mail-Einrichtung**:
   a) Wählen Sie in der Liste **Einstellungen für** den Eintrag **Exchange Web Services** aus.
   b) Geben Sie im Feld **Exchange Web Services-Adresse** die URL des Exchange Web Services-Endpunktes an.

      Diese URL gibt den Speicherort der Datei „exchange.asmx" auf dem Exchange Server an, der die Client Access Serverfunktion ausführt. Beispiel: https://CAServer.domain.com/EWS/exchange.asmx

   c) Geben Sie unter **Postfach-Anmeldeinformationen** den Benutzernamen und das Kennwort des Postfachs an, über das Quest One ActiveRoles E-Mails sendet und empfängt.

      Erstellen Sie ein Postfach auf einem Exchange 2007- oder Exchange 2010-Postfachserver für die exklusive Verwendung durch Quest One ActiveRoles, und geben Sie den Benutzernamen und das Kennwort des Postfachbenutzers an.

   d) Überprüfen Sie die von Ihnen konfigurierten Einstellungen. Klicken Sie auf **Einstellungen überprüfen**, geben Sie eine gültige E-Mail-Adresse ein und klicken Sie dann auf **Senden**.

      Hierdurch sendet Quest One ActiveRoles eine Diagnose-E-Mail-Nachricht an die von Ihnen angegebene Adresse. Es wird versucht, die Nachricht mit Hilfe von Exchange Web Services ausgehend vom Quest One ActiveRoles-Postfach zu senden. Sie können in dem Postfach mit der von Ihnen angegebenen Adresse prüfen, ob die Diagnose-Nachricht empfangen wurde.

4. Überprüfen Sie, ob die Option **Senden einer Genehmigungsantwort per E-Mail** auf der Registerkarte **E-Mail-Einrichtung** aktiviert ist.
5. Klicken Sie danach auf **OK**, um das Dialogfeld **Standardmäßige Eigenschaften der E-Mail-Einstellungen** zu schließen.

Automatisierungs-Arbeitsablauf

Als Arbeitsablauf wird eine Folge von Aktionen bezeichnet, die zum Abschluss einer bestimmten Aufgabe führen. Die Folge wird gemäß einer Reihe von Regeln oder Richtlinien ausgeführt. Ein Arbeitsablauf kann so konfiguriert werden, dass er bei einer Änderungsanforderung gestartet wird, die die Startbedingungen des Arbeitsablaufs erfüllt. Beispiel: Ein Arbeitsablauf, der den Prozess der Genehmigung bestimmter Änderungen an Verzeichnisdaten wie etwa die Erstellung neuer Benutzer oder das Füllen von Sicherheitsgruppen koordiniert. In Quest One ActiveRoles wird diese Art von Arbeitsablauf als *Änderungs-Arbeitsablauf* bezeichnet.

Ein Arbeitsablauf kann den Zweck haben, einige routinemäßige administrative Aufgaben auf regelmäßiger Basis oder bei Anforderung durch den Benutzer durchzuführen. In diesem Fall ist der Arbeitsablauf an keine Änderungsanforderung gebunden. Mit Quest One ActiveRoles können Sie einen Arbeitsablauf konfigurieren, der bestimmte Aktionen zu einem bestimmten Zeitpunkt ausführt. Sie können außerdem Benutzern ermöglichen, jederzeit auf Anforderung einen Arbeitsablauf auszuführen. Diese Arbeitsablaufkategorie wird als *Automatisierungs-Arbeitsablauf* bezeichnet.

Ein Automatisierungs-Arbeitsablauf kann die Fertigstellung komplexer administrativer Aufgaben automatisieren, um Sie bei der Verwaltung großer Aufgabenmengen zu unterstützen. Er ermöglicht außerdem die Erstellung von Überprüfungen oder Einschränkungen in Verzeichnisverwaltungsprozessen, um die Konsistenz und Konformität mit Unternehmensrichtlinien und gesetzlichen Anforderungen zu gewährleisten. Durch die Verwendung von Automatisierungs-Arbeitsabläufen können Sie sicherstellen, dass Verzeichnisverwaltungsaufgaben auf konsistente und effiziente Weise durchgeführt werden.

Optionen und Startbedingungen des Arbeitsablaufs „Automatisierung"

Die Startbedingungen eines Automatisierungs-Arbeitsablaufs legen den Auslöser fest, der den Start des Arbeitsablaufs bewirkt. Sie können einen zeitbasierten Auslöser oder einen ereignisbasierten Auslöser zum Starten eines Automatisierungs-Arbeitsablaufs verwenden. Es ist außerdem möglich, einen Automatisierungs-Arbeitsablauf auf Aufforderung durch einen Benutzer zu starten.

Bei einem zeitbasierten Auslöser können Sie einen Automatisierungs-Arbeitsablauf so konfigurieren, dass er zu einer bestimmten Tageszeit startet. Sie können einen Automatisierungs-Arbeitsablauf jedoch auch so konfigurieren, dass er mehrere Male am Tag, in der Woche oder im Monat startet. Ein ereignisbasierter Auslöser ermöglicht Ihnen, einen Automatisierungs-Arbeitsablauf beim Start des ActiveRoles-Verwaltungsdienstes zu starten. Jeder Automatisierungs-Arbeitsablauf kann nur über einen Auslöser verfügen.

Um einen zeitbasierten Auslöser zu aktivieren, muss ein Automatisierungs-Arbeitsablauf mit der Option zur Ausführung des Arbeitsablaufs gemäß einem festgelegten Zeitplan konfiguriert werden. Diese Option ist auf der Seite **Optionen und Startbedingungen des Arbeitsablaufs** in dem von der Quest One ActiveRoles-Konsole bereitgestellten Workflow Designer verfügbar. Die Seite enthält eine Reihe von Optionen, die in den folgenden Abschnitten erläutert werden.

Den Arbeitsablauf nach Plan ausführen

Wenn Sie die Option **Den Arbeitsablauf nach Plan ausführen** auswählen, dann können Sie aus den folgenden Optionen zur Ausführung des Arbeitsablaufs wählen:

- **Einmalig.** Ermöglicht Ihnen die Auswahl des Datums und der Uhrzeit für die Ausführung des Arbeitsablaufs.

- **Stündlich.** Ermöglicht Ihnen die Auswahl des Datums und der Uhrzeit für die erstmalige Ausführung des Arbeitsablaufs sowie des Wiederholungsintervalls (in Stunden und Minuten) für den Arbeitsablauf. Ein Intervall von 1 Stunde führt dazu, dass der Arbeitsablauf jede Stunde ausgeführt wird, während ein Intervall von 2 Stunden dazu führt, dass der Arbeitsablauf alle zwei Stunden ausgeführt wird.
- **Täglich.** Ermöglicht Ihnen die Auswahl des Datums sowie der Uhrzeit für die erstmalige Ausführung des Arbeitsablaufs und des Wiederholungsintervalls (in Tagen) für den Arbeitsablauf. Ein Intervall von 1 führt dazu, dass der Arbeitsablauf jeden Tag ausgeführt wird, während ein Intervall von 2 dazu führt, dass der Arbeitsablauf alle zwei Tage ausgeführt wird. Der Arbeitsablauf startet jeden Tag zur angegebenen Uhrzeit.
- **Wöchentlich.** Ermöglicht Ihnen die Auswahl des Datums sowie der Uhrzeit für die erstmalige Ausführung des Arbeitsablaufs, die Auswahl der Wochentage, an denen der Arbeitsablauf ausgeführt werden soll, sowie des Wiederholungsintervalls (in Wochen) für den Arbeitsablauf. Ein Intervall von 1 führt dazu, dass der Arbeitsablauf jede Woche ausgeführt wird, während ein Intervall von 2 dazu führt, dass der Arbeitsablauf alle zwei Wochen ausgeführt wird. Der Arbeitsablauf startet an jedem angegebenen Wochentag zur angegebenen Uhrzeit.
- **Monatlich.** Ermöglicht Ihnen die Auswahl des Datums sowie der Uhrzeit für die erstmalige Ausführung des Arbeitsablaufs, die Auswahl der Monate, in denen der Arbeitsablauf ausgeführt werden soll, sowie des Tages im Monat, an dem der Arbeitsablauf ausgeführt werden soll. Sie können entweder den speziellen Tag oder das erste, zweite, dritte, vierte oder letzte Auftreten eines bestimmten Wochentages während des Monats auswählen. Der gewünschte Wochentag kann aus einer Liste ausgewählt werden.
- **Bei Start des Verwaltungsdiensts.** Führt dazu, dass der Arbeitsablauf unmittelbar nach dem Start des ActiveRoles-Verwaltungsdienstes gestartet wird. Diese Option gilt für den durch die Einstellung **Den Arbeitsablauf ausführen** angegebenen Verwaltungsdienst.

Server, der den Arbeitsablauf startet

Bei einem Start nach Plan wird der Arbeitsablauf auf einer bestimmten Instanz des ActiveRoles-Verwaltungsdienstes ausgeführt. Die Instanz wird durch die Einstellung **Den Arbeitsablauf ausführen** festgelegt. Diese Einstellung gibt den Namen des Computers an, auf dem der Verwaltungsdienst ausgeführt wird. Sie können den gewünschten Computer aus der Liste **Den Arbeitsablauf ausführen** auswählen.

Zulassen, dass der Arbeitsablauf auf Anfrage ausgeführt wird

Wenn Sie die Option **Zulassen, dass der Arbeitsablauf auf Anfrage ausgeführt wird** auswählen, können die Benutzer den Arbeitsablauf unabhängig von einem Plan manuell ausführen. Bei Auswahl dieser Option können die Benutzer den Arbeitsablauf jederzeit bei Bedarf ausführen. Ein Arbeitsablauf kann auf Aufforderung ausgehend von der Quest One ActiveRoles-Konsole oder dem Web Interface durch Anwenden des Befehls **Ausführen** auf das Arbeitsablaufdefinitionsobjekt gestartet werden. Ausführlichere Informationen finden Sie im Abschnitt Ausführen eines Automatisierungs-Arbeitsablaufs auf Anfrage weiter unten in diesem Dokument.

Quest One ActiveRoles lässt normalerweise nur die Ausführung von jeweils einer Instanz des Arbeitsablaufs zu. Sie können dieses Verhalten jedoch für die Ausführung des Arbeitsablaufs auf Aufforderung ändern. Die folgenden Optionen sind verfügbar:

- Wenn der Arbeitsablauf bereits ausgeführt wird, dann starten Sie keine neue Instanz.
- Wenn der Arbeitsablauf bereits ausgeführt wird und eine neue Instanz auf Aufforderung gestartet wird, dann führen Sie die neue Instanz parallel aus.

Die zweite Option ermöglicht den Start einer neuen Instanz des Arbeitsablaufs auf Aufforderung, selbst wenn der Arbeitsablauf bereits ausgeführt wird. Diese Option gilt nur für die Ausführung des Arbeitsablaufs auf Aufforderung. Bei einer geplanten Ausführung lässt Quest One ActiveRoles die Ausführung von nur jeweils einer Instanz des Arbeitsablaufs zu.

„Ausführen als"-Optionen

Die Option „Ausführen als" legt das Benutzerkonto fest, unter dem der Arbeitsablauf ausgeführt wird. Klicken Sie auf die Verknüpfung **Optionen für „Ausführen als"** auf der Seite **Optionen und Startbedingungen des Arbeitsablaufs**, um die Kontoeinstellungen anzuzeigen bzw. zu ändern.

Bei einem Start nach Plan wird der Arbeitsablauf unter dem Konto des ActiveRoles-Verwaltungsdienstes, der den Arbeitsablauf ausführt, gestartet. Der Verwaltungsdienst wird gemäß der Einstellung **Den Arbeitsablauf ausführen** ausgewählt.

Bei einem Start auf Aufforderung wird der Arbeitsablauf abhängig von der Einstellung **Optionen für „Ausführen als"** unter einem der folgenden Konten ausgeführt:

- **Das Dienstkonto von Quest One ActiveRoles.** Der Arbeitsablauf wird unter dem Konto des Verwaltungsdienstes ausgeführt, der für den Start des Arbeitsablaufs auf Aufforderung verwendet wurde.
- **Konto des Benutzers, der den Arbeitsablauf gestartet hat.** Der Arbeitsablauf wird unter dem Windows-Konto des Benutzers ausgeführt, der den Arbeitsablauf auf Aufforderung gestartet hat.

Alle Aktivitäten innerhalb des Arbeitsablaufs werden normalerweise unter dem Konto ausgeführt, das von der Option „Ausführen als" für den Arbeitsablauf angegeben ist. Jede Aktivität kann jedoch so konfiguriert werden, dass Sie individuelle Optionen für „Ausführen als" verwendet. Die Eigenschaftsseite für die Aktivität enthält die Verknüpfung **Optionen für „Ausführen als"**, die es Ihnen ermöglicht, die Arbeitsablaufeinstellung „Ausführen als" auf der Basis der einzelnen Aktivitäten zu übergehen.

Bei Ausführung unter dem Konto des Verwaltungsdienstes haben die Arbeitsablaufaktivitäten dieselben Rechte und Berechtigungen wie der Verwaltungsdienst selbst und können somit jegliche Aufgaben ausführen, die für den Verwaltungsdienst zulässig sind.

Bei Ausführung unter dem Konto des Benutzers, der den Arbeitsablauf gestartet hat, können die Aktivitäten nur die Aufgaben durchführen, die Quest One ActiveRoles für dieses Benutzerkonto zulässt. Der Verwaltungsdienst verarbeitet die Aktivitäts-Vorgangsanforderung, als wenn diese von diesem Benutzer über eine ActiveRoles Benutzeroberfläche gesendet wurden, so dass die Aktivitäten über die Rechte und Berechtigungen verfügen, die dem Benutzerkonto in Quest One ActiveRoles gewährt wurden.

Genehmigung erzwingen

Die Option **Genehmigung erzwingen** legt fest, ob Genehmigungsregeln auf die vom Änderungen angewandt werden sollen, die von dem Arbeitsablauf angefordert wurden, der unter einem privilegierten Konto ausgeführt wird. Durch diese Auswahl dieser Option können die von den Aktivitäten „Arbeitsablauf" angeforderten Änderungen, deren Genehmigung noch aussteht, unabhängig von dem Konto, unter welchem der Arbeitsablauf ausgeführt wird, zur Genehmigung eingereicht werden. Andernfalls werden die Änderungen angewandt, ohne die Genehmigung abzuwarten, wenn der Arbeitsablauf unter dem Dienstkonto von Quest One ActiveRoles, dem Konto der genehmigenden Instanz oder des Quest One ActiveRoles-Verwalters ausgeführt wird. Diese Option kann je nach Aktivität überschrieben werden.

Zusätzliche Einstellungen

Die zusätzlichen Einstellungen geben an, ob der Arbeitsablauf beendet werden soll, wenn er über einen bestimmten Zeitraum hinaus ausgeführt wird. Klicken Sie auf die Verknüpfung **Zusätzliche Einstellungen** auf der Seite **Optionen und Startbedingungen des Arbeitsablaufs**, um die folgende Einstellung anzuzeigen bzw. zu ändern.

- **Den Arbeitsablauf beenden, wenn er länger dauert als:** <Zeitraum>

Diese Einstellung ermöglicht Ihnen, die Dauer einzuschränken, wie lange der Arbeitsablauf ausgeführt werden darf. Nutzen Sie diese Einstellung, um den Automatisierungs-Arbeitsablauf einzuschränken, dessen Ausführung einen langen Zeitraum benötigen würde, was zu Unannehmlichkeiten für den Benutzer führen würde.

Parameter

Wenn Sie Arbeitsablaufoptionen und Startbedingungen für einen Automatisierungs-Arbeitsablauf konfigurieren, können Sie Arbeitsablaufparameter einrichten und diesen dann Werte zuweisen. Die Parameterwerte werden während des Arbeitsablaufs von den Aktivitäten „Arbeitsablauf" verwendet. Eine Aktivität kann den Wert des gewünschten Parameters abfragen und die Aktion abhängig vom Parameterwert durchführen.

Standardmäßig sind für den Arbeitsablauf keine Parameters definiert. Auf der Seite **Parameter** können Sie Parameterdefinitionen hinzufügen, ändern (bearbeiten) oder entfernen. Wenn die Definition eines Parameters zum Arbeitsablauf hinzugefügt wurde, können Sie:

- dem Parameter einen Wert zuweisen. Wählen Sie hierzu den **Parameter** aus der Liste auf der Seite Parameter aus und klicken Sie dann auf die Schaltfläche **Parameterwert anzeigen oder ändern**. Der dem Parameter zugewiesene Wert wird in der Arbeitsablaufdefinition gespeichert. Die Arbeitsablaufaktivitäten können den Parameterwert aus der Arbeitsablaufdefinition abfragen, wenn der Arbeitsablauf ausgeführt wird.
- Konfigurieren Sie den Parameter so, dass der Benutzer den Parameterwert beim Starten des Arbeitsablaufs auf Aufforderung setzen kann. Wählen Sie hierzu den **Parameter** aus der Liste auf der Seite Parameter aus, klicken Sie auf die Schaltfläche **Bearbeiten** und deaktivieren Sie dann das Kontrollkästchen **Bei Beginn des On Demand-Arbeitsablaufs diesen Parameter nicht anzeigen**. ActiveRoles fordert den Benutzer auf, den Parameterwert zu setzen, wenn der Benutzer den On Demand-Arbeitsablauf startet. Der vom Benutzer gelieferte Parameterwert wird nur während der aktuellen Ausführung des Arbeitsablaufs verwendet.
- die verschiedenen Eigenschaften des Parameters anzeigen oder ändern. Wählen Sie hierzu den **Parameter** aus der Liste auf der Seite Parameter aus, klicken Sie auf die Schaltfläche **Bearbeiten** und verwenden Sie dann die Optionen im Dialogfeld **Parameterdefinition**.

Jeder Parameter verfügt über eine Anzahl von Eigenschaften, die den Parameter definieren. Hierzu zählen der Parametername, die Parameterbeschreibung, die Syntax der Parameterwerte, eine Liste der akzeptablen Parameterwerte, die Angabe, ob der Parameter einen einzelnen Wert oder mehrere Werte zulässt, und die Angabe, ob der Parameter einen Wert haben muss. Die zulässigen Werte können entweder durch eine statische Werteliste oder durch Verwendung eines Skripts angegeben werden. Im letztgenannten Fall berechnet das Skript die Liste der zulässigen Werte bei jedem Start des Arbeitsablaufs. Für die Zuweisung eines Werts zum Parameter kann ebenfalls ein Skript verwendet werden. Das Skript berechnet bei jedem Start des Arbeitsablaufs den Wert.

Weitere Informationen über Arbeitsablaufparameter finden Sie im Abschnitt Workflow-Parameter konfigurieren weiter oben in diesem Dokument.

Verwenden des Automatisierungs-Arbeitsablaufs

Dieser Abschnitt enthält Informationen und schrittweise Anweisungen zur Verwaltung von Automatisierungs-Arbeitsabläufen auf der Quest One ActiveRoles-Benutzeroberfläche. Folgende Themen werden erörtert:

- Erstellen einer Arbeitsablaufdefinition
- Konfigurieren der Startbedingungen für einen Automatisierungs-Arbeitsablauf
- Hinzufügen von Aktivitäten zu einem Automatisierungs-Arbeitsablauf
- Ausführen eines Automatisierungs-Arbeitsablaufs auf Anfrage
- Anzeigen des Ausführungsverlaufs eines Automatisierungs-Arbeitsablaufs
- Beenden eines laufenden Automatisierungs-Arbeitsablaufs
- Deaktivieren der Ausführung eines Automatisierungs-Arbeitsablaufs
- Erneutes Aktivieren eines Arbeitsablauf zur weiteren Ausführung
- Löschen von Automatisierungs-Arbeitsablaufsaufgaben

Erstellen einer Arbeitsablaufdefinition

Die Quest One ActiveRoles-Konsole enthält den Workflow Designer zum Erstellen und Konfigurieren von Arbeitsabläufen. Zunächst erstellen Sie eine Arbeitsablaufdefinition. Dann verwenden Sie den Workflow Designer, um einen Automatisierungs-Arbeitsablauf zu erstellen und die Konfigurationsdaten in der Arbeitsablaufdefinition zu speichern.

Erstellen einer Automatisierungs-Arbeitsablaufdefinition

1. Erweitern Sie in der Quest One ActiveRoles-Konsolenstruktur den Eintrag **Configuration | Policies**, klicken Sie mit der rechten Maustaste auf **Workflow**und wählen Sie **Neu | Arbeitsablaufrichtlinie**.
2. Befolgen Sie die Anweisungen im Assistenten „Neuer Arbeitsablauf‟:
   a) Geben Sie auf der Seite **Name und Beschreibung** einen Namen und optional eine Beschreibung für den neuen Arbeitsablauf ein.
   b) Klicken Sie auf der Seite **Arbeitsablauftyp** unter **Dieser Arbeitsablauf soll starten** auf **Bei Aufforderung durch den Benutzer oder nach Plan (Automatisierungs-Arbeitsablauf)**.
   c) Klicken Sie auf der Abschlussseite auf **Fertig stellen**.

Wenn Sie eine Workflow-Definition erstellt haben, können Sie sie im Workflow-Designer öffnen, um Workflow-Aktivitäten hinzuzufügen und die Bedingungen für den Beginn des Workflows anzugeben.

Sie können Container erstellen, um verknüpfte Workflows und andere Container zu speichern. Um einen Workflow-Container zu erstellen, klicken Sie mit der rechten Maustaste auf **Workflow** in der Konsolenstruktur und wählen Sie **Neu | Container**. Um eine Automatisierungs-Ablaufdefinition in einem bestimmten Container zu erstellen, klicken Sie mit der rechten Maustaste in die Konsolenstruktur und wählen dann **Neu | Arbeitsablauf** aus.

Gehen Sie folgendermaßen vor, um eine Automatisierungs-Arbeitsablaufdefinition zu löschen: Klicken Sie in der Konsolenstruktur unter **Konfiguration | Richtlinien | Arbeitsablauf** mit der rechten Maustaste auf das Objekt, das die Arbeitsablaufdefinition angibt, und klicken Sie dann auf **Löschen**.

Konfigurieren der Startbedingungen für einen Automatisierungs-Arbeitsablauf

Die Startbedingungen eines Automatisierungs-Arbeitsablaufs legen den Auslöser fest, der den Start des Arbeitsablaufs bewirkt. Sie können einen zeitbasierten Auslöser oder einen ereignisbasierten Auslöser zum Starten eines Automatisierungs-Arbeitsablaufs verwenden. Sie können einen Arbeitsablauf auch auf Anfrage ausführen. Verwenden Sie den Workflow Designer, um die Startbedingungen für einen Arbeitsablauf anzuzeigen oder zu ändern.

Gehen Sie folgendermaßen vor, um die Startbedingungen für einen Automatisierungs-Arbeitsablauf anzuzeigen oder zu ändern:

1. Erweitern Sie in der Quest One ActiveRoles Konsolenstruktur den Eintrag **Konfiguration | Richtlinien | Arbeitsablauf**, und wählen Sie dann den Automatisierungs-Arbeitsablauf, den Sie konfigurieren möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Automatisierungs-Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.

2. Klicken Sie im Bereich „Details" auf die Schaltfläche **Optionen und Startbedingungen des Arbeitsablaufs**, um den Bereich über dem Prozessdiagramm zu erweitern, und klicken Sie dann auf die Schaltfläche **Konfigurieren**.

Dann wird die Seite **Arbeitsablaufoptionen und -startbedingungen** geöffnet, auf der Sie Folgendes anzeigen oder ändern können:

- Die Zeitplaneinstellungen, die das Ausführungsintervall des Arbeitsablaufs festlegen. Um diese Einstellungen zu aktivieren, aktivieren Sie das Kontrollkästchen **Den Arbeitsablauf nach Plan ausführen**. Hierdurch wird der Arbeitsablauf nach Plan ausgeführt, und mit Hilfe der Optionen unter dem Kontrollkästchen können Sie den Zeitplan festlegen. Ausführlichere Informationen finden Sie im Abschnitt Den Arbeitsablauf nach Plan ausführen weiter oben in diesem Dokument.
- Zulassen, dass der Arbeitsablauf auf Anfrage ausgeführt wird Durch Aktivieren des Kontrollkästchens **Zulassen, dass der Arbeitsablauf auf Anfrage ausgeführt wird** können Benutzer den Arbeitsablauf jederzeit unabhängig vom Zeitplan manuell ausführen. Ausführlichere Informationen finden Sie unter Zulassen, dass der Arbeitsablauf auf Anfrage ausgeführt wird weiter oben in diesem Dokument.
- Mit den „Ausführen als"-Optionen können Sie das Konto festlegen, unter dem der Arbeitsablauf ausgeführt wird. Klicken Sie auf die Verknüpfung **„Ausführen als"-Optionen**, um die Kontoeinstellungen anzuzeigen oder zu ändern. Ausführlichere Informationen finden Sie im Abschnitt „Ausführen als"-Optionen weiter oben in diesem Dokument.
- Gehen Sie folgendermaßen vor, um den Arbeitsablauf zu beenden, wenn die Ausführungsdauer eine bestimmte Dauer überschreitet. Klicken Sie auf die Verknüpfung **Zusätzliche Einstellungen**, um die Einstellungen anzuzeigen oder zu ändern. Ausführlichere Informationen finden Sie im Abschnitt Zusätzliche Einstellungen weiter oben in diesem Dokument.
- Beim Konfigurieren oder Starten des Arbeitsablaufs festzulegende Parameter und Weitergabe der Daten an die Arbeitsablaufaktivitäten, wenn der Arbeitsablauf ausgeführt wird. Die Daten werden als Parameterwerte dargestellt. Um einem Parameter einen bestimmten Wert zuzuweisen, klicken Sie auf die Registerkarte **Parameter**, wählen den entsprechenden Parameter aus der Liste, und klicken dann auf die Schaltfläche **Parameterwert anzeigen oder ändern**. Ausführlichere Informationen finden Sie unter Parameter weiter oben in diesem Dokument.

Klicken Sie abschließend auf **OK**, um die Seite **Arbeitsablaufoptionen und -startbedingungen** zu schließen, und klicken Sie dann im Workflow Designer auf **Änderungen speichern**.

Hinzufügen von Aktivitäten zu einem Automatisierungs-Arbeitsablauf

Die Quest One ActiveRoles-Konsole stellt den Workflow-Designer für die Erstellung und Konfiguration der Workflows bereit. Zunächst erstellen Sie eine Arbeitsablaufdefinition. Verwenden Sie dann den Workflow Designer, um den Arbeitsablauf durch Hinzufügen und Konfigurieren von Arbeitsablaufaktivitäten zu erstellen.

Gehen Sie folgendermaßen vor, um eine Aktivität zu einem Automatisierungs-Arbeitsablauf hinzuzufügen:

1. Erweitern Sie in der Quest One ActiveRoles Konsolenstruktur den Eintrag **Konfiguration | Richtlinien | Arbeitsablauf**, und wählen Sie dann den Automatisierungs-Arbeitsablauf, zu dem Sie eine Aktivität hinzufügen möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Automatisierungs-Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.
2. Ziehen Sie im Bereich „Details" die Aktivität vom linken Bereich auf das Prozessdiagramm.
3. Klicken Sie mit der rechten Maustaste auf den Namen der Aktivität auf dem Prozessdiagramm und klicken Sie dann auf **Eigenschaften**.
4. Verwenden Sie das Dialogfeld **Eigenschaften**, um die Aktivität zu konfigurieren.

Die Schritte zum Konfigurieren einer Aktivität hängen vom Aktivitätstyp ab. Hinweise zum Konfigurieren der einzelnen Aktivitätstypen finden Sie in den Themen zum Abschnitt Konfigurieren eines Arbeitsablaufs weiter oben in diesem Dokument.

Im Dialogfeld **Eigenschaften** können Sie den Namen und die Beschreibung der Aktivität ändern. Diese Einstellungen gelten für alle Aktivitäten. Der Name gibt die Aktivität im Prozessdiagramm an. Die Beschreibung wird als QuickInfo angezeigt, wenn Sie auf die entsprechende Aktivität im Prozessdiagramm zeigen.

Sie können eine Aktivität aus dem Arbeitsablauf entfernen: Klicken Sie im Prozessdiagramm mit der rechten Maustaste auf den Namen der Aktivität, und klicken Sie dann auf **Löschen**. Damit werden alle Konfigurationseinstellungen der Aktivität aus dem Arbeitsablauf gelöscht. Sie können eine Aktivität deaktivieren, ohne die Konfigurationseinstellungen zu löschen: Klicken Sie mit der rechten Maustaste auf den Namen der Aktivität und dann auf **Deaktivieren**. Quest One ActiveRoles führt die deaktivierten Aktivitäten beim Ausführen des Arbeitsablaufs nicht aus. Die Möglichkeit, eine Aktivität zu deaktivieren und nicht zu entfernen, kann nützlich sein, um die Aktivität zeitweise innerhalb des Arbeitsablaufs zu abzuschalten. Eine solche Aktivität können Sie später jederzeit wieder aktivieren, indem Sie mit der rechten Maustaste auf deren Namen und dann auf **Aktivieren** klicken.

Ausführen eines Automatisierungs-Arbeitsablaufs auf Anfrage

Ein Automatisierungs-Arbeitsablauf kann so konfiguriert werden, dass er von den Benutzern unabhängig vom Zeitplan ausgeführt werden kann. Der Arbeitsablauf kann damit auf Anfrage gestartet werden. Ein Automatisierungs-Arbeitsablauf kann nur dann auf Anfrage ausgeführt werden, wenn der Arbeitsablauf aktiviert ist und in den Arbeitsablauf-Startbedingungen die Einstellung **Zulassen, dass der Arbeitsablauf auf Anfrage ausgeführt wird** ausgewählt wurde. Informationen über das Aktivieren eines Arbeitsablaufs finden Sie im Abschnitt Erneutes Aktivieren eines Arbeitsablauf zur weiteren Ausführung. Anweisungen zum Anzeigen oder Ändern der Arbeitsablauf-Startbedingungen finden Sie im Abschnitt Konfigurieren der Startbedingungen für einen Automatisierungs-Arbeitsablauf.

Ein Automatisierungs-Arbeitsablauf auf Anfrage kann auf der Quest One ActiveRoles-Konsole oder dem Web-Interface ausgeführt werden.

Gehen Sie folgendermaßen vor, um einen Automatisierungs-Arbeitsablauf auf Anfrage auf der Quest One ActiveRoles-Konsole auszuführen:

1. Klicken Sie in der Quest One ActiveRoles-Konsolenstruktur unter **Konfiguration | Richtlinien | Arbeitsablauf** mit der rechten Maustaste auf den gewünschten Automatisierungs-Ablauf und dann auf **Ausführen**.
2. Überprüfen Sie die Arbeitsablaufparameter, wenn Sie dazu aufgefordert werden, und ändern Sie sie gegebenenfalls.
3. Klicken Sie im Bestätigungsfeld auf **OK**.

Gehen Sie folgendermaßen vor, um einen Automatisierungs-Arbeitsablauf auf Anfrage auf dem Web-Interface auszuführen:

1. Klicken Sie auf der Startseite im Web-Interface auf **Verzeichnisverwaltung**.
2. Erweitern Sie im Bereich BAUMSTRUKTUR die Verzweigung **Arbeitsablauf** und klicken Sie dann auf den Container, in dem sich der gewünschte Arbeitsablauf befindet.
3. Klicken Sie in der Liste der Arbeitsablaufnahmen rechts neben dem Bereich BAUMSTRUKTUR auf den Namen des gewünschten Arbeitsablaufs.
4. Wählen Sie den Befehl **Ausführen** aus dem Menü.
5. Überprüfen Sie die Arbeitsablaufparameter, wenn Sie dazu aufgefordert werden, und ändern Sie sie gegebenenfalls.
6. Klicken Sie im Bestätigungsfeld auf **OK**.

Quest One ActiveRoles fordert Sie zur Eingabe von Parameterwerten auf, wenn der Arbeitsablauf über Parameter verfügt, die vom Benutzer, der den Arbeitsablauf auf Aufforderung ausführt, angegeben werden müssen. Wenn der Arbeitsablauf keine Parameter umfasst, die eine Eingabe durch den Benutzer erfordern, dann startet Quest One ActiveRoles den Arbeitsablauf, ohne Sie zur Eingabe von Parameterwerten aufzufordern.

Wenn Sie einen Automatisierungs-Arbeitsablauf gestartet haben, öffnet ActiveRoles einen Ausführungsverlaufsbericht, der Ihnen ermöglicht, den Fortschritt der Ausführung des Arbeitsablaufs zu verfolgen. Der Bericht zeigt den Status der Ausführung des Arbeitsablaufs sowie Informationen über die während der Ausführung des Arbeitsablaufs durchgeführten Aktionen an. Bei einem aktuell ausgeführten Arbeitsablauf haben Sie die Möglichkeit, die Ausführung des Arbeitsablaufs durch Anklicken der Schaltfläche **Beenden** abzubrechen.

Anzeigen des Ausführungsverlaufs eines Automatisierungs-Arbeitsablaufs

Sie können den Ausführungsverlaufsbericht verwenden, um festzustellen, welche Instanzen des Automatisierungs-Arbeitsablaufs zurzeit ausgeführt werden und welche bereits abgeschlossen sind. Der Bericht zeigt den Status der Ausführung des Arbeitsablaufs (Erfolg oder Fehlschlagen) sowie die Aktivitäten, die während jeder Ausführung des Arbeitsablaufs durchgeführt wurden, an.

Nach Abschluss des Arbeitsablaufs enthält der Bericht Verlaufsinformationen über die Ausführung des Arbeitsablaufs. Für jede abgeschlossene Ausführung des Arbeitsablaufs gibt der Bericht an, wann und von wem der Arbeitsablauf gestartet wurde, wenn er abgeschlossen wurde und welche Parameterwerte verwendet wurden.

Der Bericht führt außerdem die Arbeitsablaufaktivitäten auf, die während der Ausführung des Arbeitsablaufs durchgeführt wurden. Für jede Aktivität können Sie festlegen, ob die Aktivität erfolgreich abgeschlossen wurde oder Fehler ausgegeben wurden. Bei einem Fehler enthält der Bericht eine Fehlerbeschreibung. Bei Aktivitäten, die Änderungen an Verzeichnisdaten erfordern (z.B. Aktivitäten,

die neue Objekte erstellen oder vorhandene Objekte ändern), können Sie die geforderten Änderungen im Detail überprüfen, indem Sie die Vorgangs-ID-Nummer im Ausführungsverlaufsbericht anklicken. Die Berichtsabschnitte haben den gleichen Inhalt wie die Änderungsverlaufsberichte (siehe Abschnitt Arbeitsablaufaktivität – Berichtsabschnitte im *ActiveRoles Administratorhandbuch*).

Gehen Sie folgendermaßen vor, um den Ausführungsverlauf eines Automatisierungs-Arbeitsablaufs auf der Quest One ActiveRoles-Konsole anzuzeigen:

- Klicken Sie in der Quest One ActiveRoles-Konsolenstruktur unter **Konfiguration | Richtlinien | Arbeitsablauf** mit der rechten Maustaste auf den gewünschten Automatisierungs-Ablauf und dann auf **Ausführungsverlauf**.

Gehen Sie folgendermaßen vor, um den Ausführungsverlauf eines Automatisierungs-Arbeitsablaufs auf dem Web-Interface anzuzeigen:

1. Klicken Sie auf der Startseite im Web-Interface auf **Verzeichnisverwaltung**.
2. Erweitern Sie im Bereich BAUMSTRUKTUR die Verzweigung **Arbeitsablauf** und klicken Sie dann auf den Container, in dem sich der gewünschte Arbeitsablauf befindet.
3. Klicken Sie in der Liste der Arbeitsablaufnahmen rechts neben dem Bereich BAUMSTRUKTUR auf den Namen des gewünschten Arbeitsablaufs.
4. Wählen Sie den Befehl **Ausführungsverlauf** aus dem Menü.

Beenden eines laufenden Automatisierungs-Arbeitsablaufs

Sie können einen laufenden Automatisierungs-Arbeitsablauf beenden, um zu verhindern, dass die damit verbundenen Aktionen abgeschlossen werden.

Gehen Sie folgendermaßen vor, um einen laufenden Automatisierungs-Arbeitsablauf zu beenden

- Klicken Sie auf die Schaltfläche **Beenden** auf der Seite, auf welcher der Ausführungsverlauf des Arbeitsablaufs angezeigt wird.

  Anweisungen für den Zugriff auf den Ausführungsverlauf finden Sie im Abschnitt Anzeigen des Ausführungsverlaufs eines Automatisierungs-Arbeitsablaufs.

Auf der Seite **Ausführungsverlauf** werden sowohl laufende als auch bereits abgeschlossene Instanzen des Automatisierungs-Arbeitsablaufs angezeigt. Die Schaltfläche **Beenden** ist in jeder Instanz verfügbar, die zurzeit ausgeführt wird. Nachdem Sie auf die Schaltfläche zum Beenden einer laufenden Instanz eines Automatisierungs-Arbeitsablaufs geklickt haben, kann es einen Augenblick dauern (maximal einige Minuten), bis der Arbeitsablauf beendet wird.

Durch das Beenden eines laufenden Automatisierungs-Arbeitsablaufs werden die bereits ausgeführten Arbeitsablaufaktivitäten nicht rückgängig gemacht oder abgebrochen, es wird nur verhindert, dass der Arbeitsablauf die Aktivitäten, die in Bearbeitung sind oder noch nicht gestartet wurden, weiter ausgeführt werden.

Deaktivieren der Ausführung eines Automatisierungs-Arbeitsablaufs

Wenn Sie verhindern möchten, dass ein Automatisierungs-Arbeitsablauf während einer bestimmten Zeitdauer nicht ausgeführt wird, können Sie den Arbeitsablauf deaktivieren. Sie können den Arbeitsablauf später wieder aktivieren, damit er ausgeführt werden kann. Weitere Informationen finden Sie unter Erneutes Aktivieren eines Arbeitsablauf zur weiteren Ausführung.

Gehen Sie folgendermaßen vor, um die Ausführung eines Automatisierungs-Arbeitsablaufs zu deaktivieren:

- Klicken Sie in der Quest One ActiveRoles-Konsolenstruktur unter **Konfiguration | Richtlinien | Arbeitsablauf** mit der rechten Maustaste auf den gewünschten Automatisierungs-Ablauf und dann auf **Arbeitsablauf deaktivieren**.

Erneutes Aktivieren eines Arbeitsablauf zur weiteren Ausführung

Einen Automatisierungs-Ablauf, den Sie deaktiviert haben, damit er nicht weiter ausgeführt werden kann, können Sie anschließend wieder aktivieren, damit er auf Anforderung oder nach Zeitplan ausgeführt werden kann.

Gehen Sie folgendermaßen vor, um die Ausführung eines Automatisierungs-Arbeitsablaufs wieder zu aktivieren:

- Klicken Sie in der Quest One ActiveRoles-Konsolenstruktur unter **Konfiguration | Richtlinien | Arbeitsablauf** mit der rechten Maustaste auf den gewünschten Automatisierungs-Ablauf und dann auf **Arbeitsablauf aktivieren**.

Löschen von Automatisierungs-Arbeitsablaufsaufgaben

Quest One ActiveRoles bietet eine Reihe von Zugriffsvorlagen, die es dem Administrator ermöglichen, die folgenden, im Zusammenhang mit dem Automatisierungs-Arbeitsablauf stehenden Aufgaben zu delegieren:

- **Automatisierungs-Arbeitsablauf konfigurieren.** Um diese Aufgabe auszuführen, benötigt der delegierte Administrator Vollzugriff auf die Automatisierungs-Arbeitsablaufdefinitionen, einschließlich der Möglichkeit zum Hinzufügen, Konfigurieren und Entfernen von Arbeitsablaufdefinitionen, Anzeigen und Ändern der Arbeitsablauf-Startbedingungen, Hinzufügen und Entfernen der Arbeitsablaufparameter und Zuweisen von Werten an die Arbeitsablaufparameter.
- **Automatisierungs-Arbeitsablauf ausführen.** Um diese Aufgabe auszuführen, benötigt der delegierte Administrator die Rechte zum Anzeigen der Definition eines Automatisierungs-Arbeitsablaufs, Ausführen des Automatisierungs-Arbeitsablaufs auf Anfrage und Anzeigen des Ausführungsverlaufs des Automatisierungs-Arbeitsablaufs.
- **Ausführungsverlauf anzeigen.** Um diese Aufgabe auszuführen, benötigt der delegierte Administrator die Rechte zum Anzeigen der Definition eines Automatisierungs-Arbeitsablaufs sowie zum Anzeigen von Ausführungsverlaufsberichten über laufende und bereits abgeschlossene Instanzen des Automatisierungs-Arbeitsablaufs.

Dieser Abschnitt enthält Anweisungen zum Delegieren dieser Aufgaben an normale Benutzer oder Gruppen, die über keine Administratorrechte für Quest One ActiveRoles verfügen.

Zulassen des Zugriffs auf Arbeitsablaufcontainer

Die Ausführung von Arbeitsablaufaufgaben erfordert den Zugriff auf Container, in denen Objekte von Arbeitsablaufdefinitionen enthalten sind. In ActiveRoles haben authentifizierte Benutzer direkten Zugriff auf den Container **Konfiguration/Richtlinien/Arbeitsablauf**. Sie können entsprechende Benutzer oder Gruppen zum Anzeigen von Containern im **Arbeitsablauf**-Container berechtigen, indem Sie die Zugriffsvorlage **Arbeitsablauf – Arbeitsablaufcontainer anzeigen** auf diesen Container anwenden.

Gehen Sie folgendermaßen vor, um Arbeitsablaufcontainer anzuzeigen:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Konfiguration | Richtlinien**, klicken Sie mit der rechten Maustaste auf den **Arbeitsablauf**-Container, und klicken Sie dann auf **Kontrolle delegieren**.
2. Klicken Sie im Dialogfeld **Quest One ActiveRoles Sicherheit** auf **Hinzufügen**, um den Assistenten zum Delegieren der Kontrolle zu starten.
3. Klicken Sie auf der Seite **Benutzer oder Gruppen** im Assistenten auf **Hinzufügen** und verwenden Sie dann das Dialogfeld **Objekte auswählen**, um die gewünschten Benutzer oder Gruppen auszuwählen.
4. Aktivieren Sie im Assistenten auf der Seite **Zugriffsvorlagen** unter **Zugriffsvorlagen |** Konfiguration das Kontrollkästchen **Arbeitsablauf – Arbeitsablaufcontainer anzeigen**.
5. Befolgen Sie die Anweisungen des Assistenten und übernehmen Sie die Standardeinstellungen.
6. Klicken Sie auf **OK** im Dialogfeld **Quest One ActiveRoles-Sicherheit**.

Delegieren des Vollzugriffs auf Automatisierungs-Arbeitsabläufe

Durch die Erteilung eines Vollzugriffs auf einen Automatisierungs-Arbeitsablauf an einen Benutzer oder eine Gruppe erteilen Sie diesem Benutzer oder dieser Gruppe die Befugnis zur Durchführung der folgenden Aufgaben:

- Anzeigen der Arbeitsablaufdefinition
- Vornehmen von Änderungen am Arbeitsablauf
- Ausführen des Arbeitsablaufs
- Anzeigen des Ausführungsverlaufsberichts des Arbeitsablaufs

Sie können den Vollzugriff auf alle Automatisierungs-Arbeitsabläufe delegieren, die sich in einem bestimmten Container befinden, indem Sie die Zugriffsvorlage **Automatisierungs-Arbeitsablauf – Vollzugriff** auf diesen Container anwenden.

Gehen Sie folgendermaßen vor, um den Vollzugriff auf alle Automatisierungs-Arbeitsabläufe zu delegieren, die sich in einem bestimmten Container befinden

1. Klicken Sie in der Konsolenstruktur unter **Konfiguration | Richtlinien | Arbeitsablauf** mit der rechten Maustaste auf den gewünschten Container, und klicken Sie dann auf **Kontrolle delegieren**.
2. Klicken Sie im Dialogfeld **Quest One ActiveRoles Sicherheit** auf **Hinzufügen**, um den Assistenten zum Delegieren der Kontrolle zu starten.
3. Klicken Sie auf der Seite **Benutzer oder Gruppen** im Assistenten auf **Hinzufügen** und verwenden Sie dann das Dialogfeld **Objekte auswählen**, um die gewünschten Benutzer oder Gruppen auszuwählen.
4. Aktivieren Sie im Assistenten auf der Seite **Zugriffsvorlagen** unter **Zugriffsvorlagen | Konfiguration** das Kontrollkästchen **Automatisierungs-Arbeitsablauf – Vollzugriff**.

5. Befolgen Sie die Anweisungen des Assistenten und übernehmen Sie die Standardeinstellungen.
6. Klicken Sie auf **OK** im Dialogfeld **Quest One ActiveRoles-Sicherheit**.

Durch Anwenden der Zugriffsvorlage auf das Arbeitsablaufdefinitionsobjekt kann auch der Vollzugriff auf einen einzelnen Automatisierungs-Arbeitsablauf delegiert werden.

Gehen Sie folgendermaßen vor, um den Vollzugriff auf einen einzelnen Automatisierungs-Arbeitsablauf zu delegieren:

1. Wählen Sie im Menü **Ansicht** die Option **Erweiterte Detailansicht**.
2. Wählen Sie in der Konsolenstruktur unter **Konfiguration | Richtlinien | Arbeitsablauf** den Container, in dem das gewünschte Arbeitsablaufdefinitionsobjekt enthalten ist.
3. Wählen Sie im oberen Detailbereich das Arbeitsablaufdefinitionsobjekt aus.
4. Klicken Sie im unteren Teil des Detailbereichs auf der Registerkarte **ActiveRoles-Sicherheit** mit der rechten Maustaste auf einen leeren Bereich, und klicken Sie dann auf **Hinzufügen**, um den Assistenten zum Delegieren der Kontrolle zu starten.
5. Klicken Sie auf der Seite **Benutzer oder Gruppen** im Assistenten auf **Hinzufügen** und verwenden Sie dann das Dialogfeld **Objekte auswählen**, um die gewünschten Benutzer oder Gruppen auszuwählen.
6. Aktivieren Sie im Assistenten auf der Seite **Zugriffsvorlagen** unter **Zugriffsvorlagen | Konfiguration** das Kontrollkästchen **Automatisierungs-Arbeitsablauf – Vollzugriff**.
7. Befolgen Sie die Anweisungen des Assistenten und übernehmen Sie die Standardeinstellungen.

Delegieren der Aufgabe zum Ausführen eines Automatisierungs-Arbeitsablaufs

Sie können Benutzer oder Gruppen zum Ausführen aller Automatisierungs-Arbeitsabläufe berechtigen, die sich in einem bestimmten Container befinden, indem Sie die Zugriffsvorlage **Automatisierungs-Arbeitsablauf – Anzeigen und ausführen** auf diesen Container anwenden. Dadurch können Benutzer oder Gruppen den Automatisierungs-Arbeitsablauf zwar ausführen, aber keine Änderungen am Arbeitsablauf vornehmen.

Gehen Sie folgendermaßen vor, um das Ausführen von Automatisierungs-Arbeitsabläufen zu delegieren, die sich in einem bestimmten Container befinden:

1. Klicken Sie in der Konsolenstruktur unter **Konfiguration | Richtlinien | Arbeitsablauf** mit der rechten Maustaste auf den gewünschten Container, und klicken Sie dann auf **Kontrolle delegieren**.
2. Klicken Sie im Dialogfeld **Quest One ActiveRoles Sicherheit** auf **Hinzufügen**, um den Assistenten zum Delegieren der Kontrolle zu starten.
3. Klicken Sie auf der Seite **Benutzer oder Gruppen** im Assistenten auf **Hinzufügen** und verwenden Sie dann das Dialogfeld **Objekte auswählen**, um die gewünschten Benutzer oder Gruppen auszuwählen.
4. Aktivieren Sie im Assistenten auf der Seite **Zugriffsvorlagen** unter **Zugriffsvorlagen | Konfiguration** das Kontrollkästchen **Automatisierungs-Arbeitsablauf – Anzeigen und ausführen**.
5. Befolgen Sie die Anweisungen des Assistenten und übernehmen Sie die Standardeinstellungen.
6. Klicken Sie auf **OK** im Dialogfeld **Quest One ActiveRoles-Sicherheit**.

Durch Anwenden der Zugriffsvorlage auf das Arbeitsablaufdefinitionsobjekt können Benutzer oder Gruppen auch zum Ausführen eines einzelnen Automatisierungs-Arbeitsablaufs berechtigt werden.

Gehen Sie folgendermaßen vor, um die Aufgabe zum Ausführen eines einzelnen Automatisierungs-Arbeitsablaufs zu delegieren:

1. Wählen Sie im Menü **Ansicht** die Option **Erweiterte Detailansicht**.
2. Wählen Sie in der Konsolenstruktur unter **Konfiguration | Richtlinien | Arbeitsablauf** den Container, in dem das gewünschte Arbeitsablaufdefinitionsobjekt enthalten ist.
3. Wählen Sie im oberen Detailbereich das Arbeitsablaufdefinitionsobjekt aus.
4. Klicken Sie im unteren Teil des Detailbereichs auf der Registerkarte **ActiveRoles-Sicherheit** mit der rechten Maustaste auf einen leeren Bereich, und klicken Sie dann auf **Hinzufügen**, um den Assistenten zum Delegieren der Kontrolle zu starten.
5. Klicken Sie auf der Seite **Benutzer oder Gruppen** im Assistenten auf **Hinzufügen** und verwenden Sie dann das Dialogfeld **Objekte auswählen**, um die gewünschten Benutzer oder Gruppen auszuwählen.
6. Aktivieren Sie im Assistenten auf der Seite **Zugriffsvorlagen** unter **Zugriffsvorlagen | Konfiguration** das Kontrollkästchen **Automatisierungs-Arbeitsablauf – Anzeigen und ausführen**.
7. Befolgen Sie die Anweisungen des Assistenten und übernehmen Sie die Standardeinstellungen.

Delegieren der Aufgabe zum Anzeigen des Ausführungsverlaufs eines Automatisierungs-Arbeitsablaufs

Sie können Benutzer oder Gruppen zum Anzeigen des Ausführungsverlaufs aller Automatisierungs-Arbeitsabläufe berechtigen, die sich in einem bestimmten Container befinden, indem Sie die Zugriffsvorlage **Automatisierungs-Arbeitsablauf – Anzeigen** auf diesen Container anwenden. Dadurch können Benutzer oder Gruppen den Ausführungsverlauf eines Automatisierungs-Arbeitsablaufs zwar anzeigen, aber den Arbeitsablauf weder ändern noch ausführen.

Gehen Sie folgendermaßen vor, um das Anzeigen des Ausführungsverlaufs aller Automatisierungs-Arbeitsabläufe zu delegieren, die sich in einem bestimmten Container befinden:

1. Klicken Sie in der Konsolenstruktur unter **Konfiguration | Richtlinien | Arbeitsablauf** mit der rechten Maustaste auf den gewünschten Container, und klicken Sie dann auf **Kontrolle delegieren**.
2. Klicken Sie im Dialogfeld **Quest One ActiveRoles Sicherheit** auf **Hinzufügen**, um den Assistenten zum Delegieren der Kontrolle zu starten.
3. Klicken Sie auf der Seite **Benutzer oder Gruppen** im Assistenten auf **Hinzufügen** und verwenden Sie dann das Dialogfeld **Objekte auswählen**, um die gewünschten Benutzer oder Gruppen auszuwählen.
4. Aktivieren Sie im Assistenten auf der Seite **Zugriffsvorlagen** unter **Zugriffsvorlagen | Konfiguration** das Kontrollkästchen **Automatisierungs-Arbeitsablauf – Anzeigen**.
5. Befolgen Sie die Anweisungen des Assistenten und übernehmen Sie die Standardeinstellungen.
6. Klicken Sie auf **OK** im Dialogfeld **Quest One ActiveRoles-Sicherheit**.

Durch Anwenden der Zugriffsvorlage auf das Arbeitsablaufdefinitionsobjekt können Benutzer oder Gruppen auch zum Anzeigen des Ausführungsverlaufs eines einzelnen Automatisierungs-Arbeitsablaufs berechtigt werden.

Gehen Sie folgendermaßen vor, um die Aufgabe zum Anzeigen des Ausführungsverlaufs eines einzelnen Automatisierungs-Arbeitsablaufs zu delegieren:

1. Wählen Sie im Menü **Ansicht** die Option **Erweiterte Detailansicht**.
2. Wählen Sie in der Konsolenstruktur unter **Konfiguration | Richtlinien | Arbeitsablauf** den Container, in dem das gewünschte Arbeitsablaufdefinitionsobjekt enthalten ist.
3. Wählen Sie im oberen Detailbereich das Arbeitsablaufdefinitionsobjekt aus.
4. Klicken Sie im unteren Teil des Detailbereichs auf der Registerkarte **ActiveRoles-Sicherheit** mit der rechten Maustaste auf einen leeren Bereich, und klicken Sie dann auf **Hinzufügen**, um den Assistenten zum Delegieren der Kontrolle zu starten.
5. Klicken Sie auf der Seite **Benutzer oder Gruppen** im Assistenten auf **Hinzufügen** und verwenden Sie dann das Dialogfeld **Objekte auswählen**, um die gewünschten Benutzer oder Gruppen auszuwählen.
6. Aktivieren Sie im Assistenten auf der Seite **Zugriffsvorlagen** unter **Zugriffsvorlagen | Konfiguration** das Kontrollkästchen **Automatisierungs-Arbeitsablauf – Anzeigen**.
7. Befolgen Sie die Anweisungen des Assistenten und übernehmen Sie die Standardeinstellungen.

Aktivitätserweiterungen

In Quest One ActiveRoles können die Administratoren die Workflow-Aktivitäten der vordefinierten Typen, die mit Quest One ActiveRoles installiert sind, konfigurieren. Standardmäßig enthält die Liste der Aktivitäten in Workflow Designer nur die vordefinierten Aktivitätstypen wie etwa **Genehmigungsaktivität** oder **Benachrichtigungsaktivität**. Es ist möglich, die Liste durch Hinzufügen neuer Aktivitäten zu erweitern.

Jeder Aktivitätstyp bestimmt einen bestimmten Workflow-Vorgang (z.B. Ursprung einer Genehmigungsaufgabe oder einer Benachrichtigung) zusammen mit einer Sammlung von Aktivitätsparametern, um den Workflow-Vorgang zu konfigurieren (z.B. Parameter, die die genehmigenden Personen oder die Empfänger der Benachrichtigungen festlegen). Quest One ActiveRoles baut durch die Möglichkeit, benutzerdefinierte Typen von Workflow-Aktivitäten zu implementieren und bereit zu stellen, auf diesem Konzept auf. ActiveRoles Server ermöglicht die Erstellung von benutzerdefinierten Aktivitätstypen sowie die Auflistung in Workflow Designer zusammen mit den vordefinierten Aktivitätstypen, was den Administratoren ermöglicht, Arbeitsablaufaktivitäten zu konfigurieren, die von diesen neuen Aktivitätstypen festgelegte benutzerdefinierte Vorgänge durchführen.

Quest One ActiveRoles ermöglicht die Erstellung von benutzerdefinierten Aktivitäten auf Grundlage dem integrierten **Script-Activity**-Aktivitätstypen. Die Erstellung und Konfiguration einer Skriptaktivität von Grund auf kann jedoch zeitaufwendig sein. Benutzerdefinierte Aktivitätstypen bieten eine Möglichkeit, dieses zeitaufwendige Verfahren abzukürzen. Sobald ein benutzerdefinierter Aktivitätstyp bereitgestellt ist, der auf ein bestimmtes Skript verweist, können Administratoren auf einfache Weise Arbeitsablaufaktivitäten dieses Typs konfigurieren und anwenden, sodass diese Aktivitäten die von diesem Skript vorgegebenen Vorgänge ausführen. Das Aktivitätsskript definiert auch die für den Aktivitätstyp spezifischen Aktivitätsparameter.

Benutzerdefinierte Aktivitätstypen bieten einen erweiterbaren Mechanismus für die Bereitstellung von benutzerdefinierten Arbeitsablaufaktivitäten. Diese Möglichkeit wird über die Objektklasse „Richtlinientyp" implementiert. Richtlinientypobjekte können mit Hilfe der Quest One ActiveRoles-Konsole erstellt werden, wobei jedes Objekt einen bestimmten Typ der benutzerdefinierten Workflow-Aktivität darstellt.

Designelemente

Die Erweiterungsfähigkeit von Arbeitsablaufaktivitätstypen stützt sich auf zwei Interaktionen: Aktivitätstyp-Bereitstellung und Aktivitätstyp-Nutzung.

Aktivitätstyp-Bereitstellung

Der Bereitstellungsprozess beinhaltet die Entwicklung eines Skripts, das den Workflow-Vorgang implementiert und die Akvititätsparameter erklärt; die Erstellung eines Skriptmoduls, das dieses Skript enthält; und die Erstellung eines Richtlinientyps, der sich auf dieses Skriptmodul bezieht. Um einen Aktivitätstyp in einer anderen Umgebung bereitzustellen, können Sie den Aktivitätstyp in eine Exportdatei in der Quellumgebung exportieren und die Datei dann in die Zielumgebung importieren. Die Verwendung von Exportdateien erleichtert die Verbreitung von benutzerdefinierten Aktivitätstypen.

Aktivitätstyp-Nutzung

Die Aktivitätstyp-Nutzung ist der Prozess der Konfiguration von Arbeitsablaufaktivitäten. Sie erfolgt immer dann, wenn Sie eine Aktivität zu einem Arbeitsablauf in Workflow Designer hinzufügen. Um eine Aktivität zu einem Arbeitsablauf hinzuzufügen, ziehen Sie den gewünschten Aktivitätstyp von der Toolbox auf das Arbeitsablaufprozessdiagramm. Die Toolbox, die sich auf der linken Seite des Diagramms befindet, enthält alle in Quest One

ActiveRoles definierten Aktivitätstypen, einschließlich der benutzerdefinierten. Für jede benutzerdefinierte Aktivität bietet Workflow Designer eine Seite für die Konfiguration der für diesen Aktivitätstyp spezifischen Aktivitätsparameter an. Nach der Konfiguration der Aktivitätsparameter enthält der Arbeitsablauf eine voll funktionsfähige Aktivität des ausgewählten benutzerdefinierten Typs.

Quest One ActiveRoles stellt eine vollständige graphische Benutzerschnittstelle mit einer Programmierschnittstellen zur Erstellung und Verwaltung benutzerdefinierter Aktivitätstypen zur Verfügung. Mit Hilfe dieser Schnittstelle können Quest One ActiveRoles Workflows erweitert werden, um die Bedürfnisse einer bestimmten Umgebung zu erfüllen. Quest One ActiveRoles hat auch einen Bereitstellungsmechanismus, mit dessen Hilfe die Administratoren neue Arten der Workflow-Aktivität in den Vorgang einbringen können.

Da die Erweiterung der Workflow-Aktivität zwei Interaktionen beinhaltet, stellt Quest One ActiveRoles Lösungen auf beiden Gebieten bereit. Der Verwaltungsdienst verwaltet die Definitionen der Aktivitätstypen, wobei er die Aktivitätstypen seinen Clients verfügbar macht, z.B. Quest One ActiveRoles-Konsole oder ADSI Provider. Die Konsole kann für folgende Vorgänge verwendet werden:

- Erstellen eines neuen benutzerdefinierten Aktivitätstyps, entweder von Grund auf oder per Import eines Aktivitätstyps, der aus einer anderen Umgebung exportiert wurde.
- Vornehmen von Änderungen an der Definition eines vorhandenen benutzerdefinierten Aktivitätstyps.
- Hinzufügen einer Aktivität eines bestimmten benutzerdefinierten Typs zu einem Arbeitsablauf, wodurch die erforderlichen Änderungen an den von der Aktivitätstypdefinition bereitgestellten Aktivitätsparametern vorgenommen werden.

Normalerweise entwickelt ein Quest One ActiveRoles-Experte einen benutzerdefinierten Aktivitätstyp in einer separaten Umgebung und exportiert den Aktivitätstyp dann in eine Exportdatei. Ein Quest One ActiveRoles-Administrator stellt den Aktivitätstyp in der Produktionsumgebung bereit, indem er die Exportdatei importiert. Anschließend kann Workflow Designer für die Konfiguration und Anwendung der Aktivitäten dieses neuen Typs verwendet werden.

Richtlinientypobjekte

Die Erweiterungsfähigkeit der Arbeitsablaufaktivitätstyp stützt sich auf Richtlinientypobjekte der Kategorie „Arbeitsablaufaktivität", von denen jedes einen einzigen Arbeitsablaufaktivitätstyp darstellt. Richtlinientypobjekte werden sowohl bei der Aktivitätstyp-Bereitstellung als auch bei der Aktivitätstyp-Nutzung verwendet. Der Prozess der Bereitstellung eines neuen Aktivitätstyps umfasst die Erstellung eines Richtlinientypobjekts. Während des Hinzufügens einer benutzerdefinierten Aktivität zu einem Arbeitsablauf wird die Aktivitätstypdefinition vom entsprechenden Richtlinientypobjekt abgerufen.

Jedes Richtlinientypobjekt der Kategorie „Arbeitsablaufaktivität" enthält die folgenden Daten für die Definition eines einzelnen Aktivitätstyps:

- **Anzeigename.** Gibt den Aktivitätstyp in Workflow Designer an. Dieser Name wird in der Aktivitäten-Toolbox angezeigt, die sich links vom Arbeitsablaufprozessdiagramm befindet.
- **Beschreibung.** Ein Text, der den Aktivitätstyp beschreibt. Dieser Text wird als eine Standardbeschreibung für jede Aktivität verwendet, die auf diesem Richtlinientypobjekt basiert.
- **Verweis auf ein Skriptmodul.** Gibt das Skriptmodul an, das von den Arbeitsablaufaktivitäten dieses Typs verwendet wird. Wenn Sie eine benutzerdefinierte Aktivität zu einem Arbeitsablauf hinzufügen, erstellen Sie effektiv eine Aktivität, die eine bestimmte Skriptfunktion aus dem Skriptmodul ausführt, das vom entsprechenden Richtlinientypobjekt angegeben wird.

- **Richtlinientypkategorie.** Die Richtlinientypobjekte, die benutzerdefinierte Arbeitsablaufaktivitäten definieren, fallen in eine separate Richtlinientypkategorie mit der Bezeichnung „Arbeitsablaufaktivität".
- **Workflow-Kategorie.** Legt fest, ob die benutzerdefinierte Aktivität nur für Änderungs-Workflows, nur für Automatisierungs-Workflows oder beide verwendet werden kann.
- **Auszuführende Funktion.** Gibt die Skriptfunktion an, die von den Arbeitsablaufaktivitäten dieses Typs ausgeführt wird. Die Funktion muss in dem für den Richtlinientyp ausgewählten Skriptmodul vorhanden sein.
- **Funktion zur Deklaration der Parameter.** Gibt die Skriptfunktion an, die die Parameter für die Arbeitsablaufaktivitäten dieses Typs deklariert. Die Funktion muss in dem für den Richtlinientyp ausgewählten Skriptmodul vorhanden sein. Standardmäßig wird vorausgesetzt, dass die Parameter von der Funktion mit der Bezeichnung „onInit" deklariert werden.
- **Richtlinientypsymbol.** Das Bild, das neben dem Anzeigenamen des Aktivitätstyps in Workflow Designer angezeigt wird, um die Identifizierung und visuelle Unterscheidung dieses Aktivitätstyps von anderen Arbeitsablaufaktivitätstypen zu erleichtern.

Um einen benutzerdefinierten Aktivitätstyp zu erstellen, müssen Sie zunächst ein Skriptmodul erstellen, das die Skriptfunktion enthält, die von den Arbeitsablaufaktivitäten dieses Typs ausgeführt wird. Dann können Sie ein Richtlinientypobjekt erstellen, das auf dieses Skriptmodul verweist. Wenn man einen Aktivitätstyp importiert, erstellt Quest One ActiveRoles automatisch das Skriptmodul und das Richtlinientypobjekt für diesen Aktivitätstyp. Nach der Erstellung des Richtlinientypobjekts können Sie eine Aktivität dieses neuen Typs zu einem Arbeitsablauf hinzufügen.

Erstellen und Verwalten von benutzerdefinierten Aktivitätstypen

In Quest One ActiveRoles stellen die Richtlinientypobjekte die Fähigkeit bereit, die Definition eines benutzerdefinierten Aktivitätstyps in einem einzelnen Objekt zu speichern. Richtlinientypobjekte können exportiert und importiert werden. Dies erleichtert die Verbreitung von benutzerdefinierten Arbeitsablaufaktivitäten in anderen Umgebungen.

In Workflow Designer wird einem Administrator eine Liste der von den Richtlinientypobjekten abgeleiteten Aktivitätstypen angezeigt. Wenn man einen benutzerdefinierten Aktivitätstyp in der Liste wählt, erstellt Quest One ActiveRoles eine Workflow-Aktivität auf Grundlage der im entsprechenden Richtlinientypobjekt gefundenen Einstellungen.

Dieser Abschnitt deckt die folgenden, für benutzerdefinierte Aktivitätstypen spezifischen Aufgaben ab:

- Erstellen eines Richtlinientypobjekts
- Ändern eines vorhandenen Richtlinientypobjekts
- Verwenden von Richtlinientypcontainern
- Exportieren von Aktivitätstypen
- Importieren von Aktivitätstypen
- Konfigurieren einer Aktivität eines benutzerdefinierten Typs
- Löschen eines Richtlinientypobjekts

Weitere Informationen über Richtlinientypobjekte einschließlich Anweisungen zur Skripterstellung für Richtlinientypobjekte erhalten Sie unter Quest One ActiveRoles SDK.

Erstellen eines Richtlinientypobjekts

Quest One ActiveRoles speichert Richtlinientypobjekte im Container **Policy Types**. Sie können auf diesen Container in der Quest One ActiveRoles-Konsole zugreifen, indem Sie den Zweig **Configuration/ Server Configuration** der Konsolenstruktur erweitern.

Gehen Sie folgendermaßen vor, um ein neues Richtlinientypobjekt zu erstellen:

1. Klicken Sie in der Konsolenstruktur unter **Configuration/Server** Configuration/Policy Types mit der rechten Maustaste auf den Richtlinientypcontainer, in dem Sie ein neues Objekt erstellen möchten, und wählen Sie dann **Neu | Richtlinientyp**.

   *Wenn Sie zum Beispiel ein neues Objekt im Root-Container erstellen möchten, klicken Sie mit der rechten Maustaste auf **Richtlinientypen**.*

2. Geben Sie im Assistenten „Neues Objekt - Richtlinientyp" einen Namen, einen Anzeigenamen und optional eine Beschreibung für das neue Objekt ein.

   Der Anzeigename gibt den Aktivitätstyp in Workflow Designer an. Der Beschreibungstext wird als eine Standardbeschreibung für jede Aktivität verwendet, die auf diesem Richtlinientypobjekt basiert.

3. Klicken Sie auf **Weiter**.
4. Klicken Sie auf **Durchsuchen** und wählen Sie das Skriptmodul, das das Skript enthält, das von Arbeitsablaufaktivitäten dieses Typs verwendet wird.

   *Das Skriptmodul muss im Container **Configuration/Script Modules** vorhanden sein.*

5. Wählen Sie im Bereich **Kategorie des Richtlinientyps** die Option **Arbeitsablaufaktivität** aus.
6. Wählen Sie aus der Liste **Auszuführende Funktion** den Namen der Skriptfunktion, die von den Arbeitsablaufaktivitäten dieses Typs ausgeführt werden.

   *Die Liste enthält die Namen aller Funktionen, die in dem von Ihnen in Schritt 4 ausgewählten Skript gefunden wurden. Jede Aktivität dieses Typs wird die Funktion ausführen, die Sie aus der Liste **Auszuführende Funktion** auswählen.*

7. Wählen Sie in der **Verwenden in**-Liste die entsprechende Option, um die Kategorie des Workflows anzugeben, in welcher die Aktivität dieses Typs verwendet werden kann:
   - **Änderungs-Workflow.** Die Aktivität kann nur in Änderungs-Workflows verwendet werden, d.h. in Workflows, die nach Vorgangsaufforderungen, die bestimmte Bestimmungen erfüllen, ausgeführt werden.
   - **Automatisierungs-Workflow.** Die Aktivität kann nur in Automatisierungs-Workflows verwendet werden, d.h. in Workflows, die nach einem Zeitplan synchronisiert oder nach einer Benutzeranforderung ausgeführt werden.
   - **Jeder Workflow.** Die Akvitiät kann für Änderungs- und Automatisierungs-Workflows verwendet werden.
8. Wählen Sie aus der Liste **Funktion zur Deklaration von Parametern** den Namen der Skriptfunktion, die die Parameter definiert, die für diesen Arbeitsablaufaktivitätstyp spezifisch sind.

   *Die Liste enthält die Namen aller Funktionen, die in dem von Ihnen in Schritt 4 ausgewählten Skript gefunden wurden. Jede Aktivität dieses Typs verfügt über die Parameter, die durch die Funktion angegeben werden, die Sie aus der Liste **Funktion zur Deklaration von Parametern** auswählen. Normalerweise ist dies eine Funktion mit der Bezeichnung „onInit" (ausführlichere Informationen finden Sie im Quest One ActiveRoles Software Development Kit (SDK)).*

9. Klicken Sie auf **Richtlinientyp-Symbol**, um das Bild anzuzeigen, das diesen Aktivitätstyp angibt. Um ein anderes Bild auszuwählen, klicken Sie auf **Ändern** und öffnen dann eine Symboldatei, die das gewünschte Bild enthält.

Dieses Bild wird neben dem Anzeigenamen des Aktivitätstyps in Workflow Designer angezeigt, um die Identifizierung und visuelle Unterscheidung dieses Aktivitätstyps von anderen Aktivitätstypen zu erleichtern.

*Das Bild wird im Richtlinientypobjekt gespeichert. In dem Dialogfeld, das durch Anklicken von **Richtlinientyp-Symbol** angezeigt wird, können Sie das aktuell verwendete Bild sehen. Um wieder das Standardbild zu verwenden, klicken Sie auf **Standardsymbol verwenden**. Wenn die Schaltfläche nicht verfügbar ist, dann wird aktuell das Standardbild verwendet.*

10. Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um die Erstellung des neuen Richtlinientypobjekts abzuschließen.

Ändern eines vorhandenen Richtlinientypobjekts

Sie können ein vorhandenes Richtlinientypobjekt ändern, indem Sie die allgemeinen Eigenschaften, das Skript oder das Symbol ändern. Die allgemeinen Eigenschaften umfassen den Namen, den Anzeigenamen und die Beschreibung. Die Richtlinientypobjekte befinden sich unter **Configuration/ Server Configuration/Policy Types** in der Quest One ActiveRoles-Konsole.

Die folgende Tabelle fasst die Änderungen zusammen, die Sie an einem vorhandenen Richtlinientypobjekt vornehmen können, vorausgesetzt, dass Sie das Objekt in der Quest One ActiveRoles-Konsole gefunden haben.

ÄNDERUNG VON	VORGEHENSWEISE	KOMMENTAR
Name des Objekts	Klicken Sie mit der rechten Maustaste auf das Objekt und klicken Sie dann auf **Umbenennen**.	Der Name wird verwendet, um das Objekt zu identifizieren, und muss für die im selben Richtlinientypcontainer enthaltenen Objekte eindeutig sein.
Anzeigename oder Beschreibung	Klicken Sie mit der rechten Maustaste auf das Objekt, klicken Sie auf **Eigenschaften** und nehmen Sie die erforderlichen Änderungen auf der Registerkarte **Allgemein** vor.	Durch die Änderung des Anzeigenamens wird auch der Name des Aktivitätstyps in Workflow Designer geändert. Sie müssen möglicherweise die Ansicht in Workflow Designer aktualisieren, damit der neue Name angezeigt wird.
Skriptmodul	Klicken Sie mit der rechten Maustaste auf das Objekt, klicken Sie auf **Eigenschaften**, dann auf die Registerkarte **Skript**, anschließend auf **Durchsuchen** und wählen Sie dann das gewünschte Skriptmodul aus.	Sie können das Skript in dem Skriptmodul ändern, das aktuell mit dem Richtlinientypobjekt verbunden ist, anstatt ein anderes Skriptmodul auszuwählen. Um das Skript anzuzeigen oder zu ändern, suchen Sie das Skript Modul in der Quest One ActiveRoles-Konsolenstruktur unter **Configuration/Script Modules** und wählen es aus. Die Änderung des Skripts beeinflusst alle vorhandenen Arbeitsablaufaktivitäten dieses Typs. Wenn Sie eine Aktivität zu einem Arbeitsablauf hinzufügen und dann das Skript für das Richtlinientypobjekt ändern, auf dessen Grundlage die Aktivität erstellt wurde, dann führt die Aktivität das geänderte Skript aus.

ÄNDERUNG VON	VORGEHENSWEISE	KOMMENTAR
Auszuführende Funktion	Klicken Sie mit der rechten Maustaste auf das Objekt, klicken Sie dann auf **Eigenschaften**, anschließend auf die Registerkarte **Skript** und wählen Sie dann die entsprechende Funktion aus der Liste **Auszuführende Funktion** aus.	Die Änderung dieser Einstellung führt dazu, dass die Aktivitäten dieses Typs die von Ihnen ausgewählte Funktion ausführen. Die Änderung der Funktion hat keinen Einfluss auf vorhandene Aktivitäten dieses Typs. Wenn Sie eine neue Aktivität dieses Typs hinzufügen, wird die Aktivität die neue Funktion ausführen.
Workflow-Kategorie	Klicken Sie mit der rechten Maustaste auf das Objekt, dann auf **Eigenschaften** und auf den **Skript**-Tab und wählen Sie die entsprechende Option in der **Verwenden in**-Liste.	Durch diese Einstellung wird die Workflow-Kategorie (Änderungs-, Automatisierungs-Workflow oder jeder Workflow) festgelegt, für welche die Aktivität dieser Art zulässig ist. Nach Änderung dieser Einstellung kann eine Aktivität dieses Typs nur zu der entsprechenden Workflow-Kategorie hinzugefügt werden. Deshalb kann, wenn Sie die Option **Änderungs-Workflow** wählen, die Aktivität dieses Typs nicht zu einem Automatisierungs-Workflow hinzugefügt werden.
Funktion zur Deklaration von Parametern	Klicken Sie mit der rechten Maustaste auf das Objekt, klicken Sie dann auf **Eigenschaften**, anschließend auf die Registerkarte **Skript**und wählen Sie dann die entsprechende Funktion aus der Liste **Funktion zur Deklaration von Parametern** aus.	Die Änderung dieser Einstellung ändert die Liste der für diesen Aktivitätstyp spezifischen Aktivitätsparameter. Die Änderungen haben keinen Einfluss auf die Parameter der vorhandenen Aktivitäten dieses Typs. Wenn Sie eine neue Aktivität dieses Typs hinzufügen, wird die Liste der Aktivitätsparameter mit Hilfe der neuen Funktion zur Deklaration von Parametern erstellt.
Richtlinientyp-Symbol	Klicken Sie mit der rechten Maustaste auf das Objekt, klicken Sie auf **Eigenschaften** und dann auf die Registerkarte **Skript**, klicken Sie anschließend auf **Richtlinientyp-Symbol** und gehen Sie dann wie nachfolgend beschrieben vor: • Klicken Sie auf **Ändern** und öffnen Sie eine Symboldatei, die das gewünschte Symbol enthält. • Klicken Sie auf **Standardsymbol verwenden**, um wieder das Standardbild zu verwenden.	Die Änderung dieser Einstellung ändert das Bild, das neben dem Anzeigenamen des Aktivitätstyps in Workflow Designer im Bereich neben dem Arbeitsablaufprozessdiagramm angezeigt wird.

Verwenden von Richtlinientypcontainern

Sie können einen Richtlinientypcontainer für die Speicherung zugehöriger Richtlinientypobjekte und anderer Richtlinientypcontainer verwenden.

Container bieten die Möglichkeit einer zusätzlichen Kategorisierung von benutzerdefinierten Aktivitätstypen und erleichtern somit das Auffinden und die Auswahl eines Aktivitätstyps in Workflow Designer. Die Aktivitäten-Toolbox neben dem Arbeitsablaufprozessdiagramm listet die benutzerdefinierten Aktivitätstypen zusammen mit den Containern in denen sich die entsprechenden

Richtlinientypobjekte befinden, auf. Um zu vermeiden, dass die Container die Aktivitäten-Toolbox überdecken, zeigt Workflow Designer nur die Container an, die dem Container **Richtlinientyp** direkt untergeordnet sind, und ignoriert die Container der darunter liegenden Ebenen. Zur Veranschaulichung dieses Verhaltens dient beispielhaft der Pfad zu einem Richtlinientypobjekt wie etwa 'Richtlinientypen/ Container A/Container B/Objekt C'. In diesem Fall zeigt Workflow Designer nur Container A und den Aktivitätstyp C unter Container A an und ignoriert Container B.

Gehen Sie folgendermaßen vor, um einen neuen Richtlinientypcontainer zu erstellen:

1. Klicken Sie in der Konsolenstruktur unter **Configuration/Server Configuration/Policy Types** mit der rechten Maustaste auf den Richtlinientypcontainer, in dem Sie einen neuen Container erstellen möchten, und wählen Sie dann **Neu | Richtlinientypcontainer**.

   *Wenn Sie zum Beispiel einen neuen Container im Root-Container erstellen möchten, klicken Sie mit der rechten Maustaste auf **Richtlinientypen**.*

2. Geben Sie im Assistenten „Neues Objekt – Richtlinientypcontainer" einen Namen und optional eine Beschreibung für den neuen Container ein.

   *Der Name des Containers wird in Workflow Designer angezeigt, wenn sich der Container direkt im Container **Richtlinientypen** befindet.*

3. Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um die Erstellung des neuen Containers abzuschließen.

Exportieren von Aktivitätstypen

Sie können Richtlinientypobjekte exportieren, damit die Definition der Aktivitätstypen in einer XML-Datei gespeichert werden kann, welche in eine andere Quest One ActiveRoles-Umgebung importiert werden kann. Das Exportieren und anschließende Importieren von Richtlinientypobjekten erleichtert die Verbreitung von benutzerdefinierten Aktivitätstypen in anderen Umgebungen.

Gehen Sie folgendermaßen vor, um ein Richtlinientypobjekt oder einen Container zu exportieren:

- Klicken Sie mit der rechten Maustaste auf das Richtlinientypobjekt oder den Container in der Quest One ActiveRoles-Konsole, klicken Sie dann auf **Exportieren** und geben Sie eine XML-Datei für die Speicherung der Exportdaten an.

Sie können mehrere zu exportierende Richtlinienobjekte auswählen oder Sie können einen Container auswählen, um alle in diesem Container befindlichen Richtlinientypobjekte und Container zu exportieren. In beiden Fällen erstellt der Exportvorgang eine einzelne XML-Datei, die später in jeden beliebigen Container unter dem Knoten **Policy Types** importiert werden kann.

Beim Export von Richtlinientypobjekten wird eine XML-Datei erstellt, die sowohl die Objekte als auch die Skriptmodule angibt, die die Skripts für jeden zu exportierenden Aktivitätstyp angibt. Während eines Imports erstellt Quest One ActiveRoles Richtlinientypobjekte und die Skriptmodule auf der Grundlage der Daten in der XML-Datei. Als Ergebnis des Imports werden Aktivitätstypen in der neuen Umgebung repliziert; diese können dann auf gleiche Weise wie in der Umgebung, aus der sie exportiert wurden, verwendet werden.

Importieren von Aktivitätstypen

Sie können die exportierten Richtlinientypobjekte und Container importieren. Hierdurch werden sie zum Richtlinientypcontainer hinzugefügt, was Ihnen ermöglicht, von diesen Richtlinientypobjekten festgelegte benutzerdefinierte Aktivitäten zu konfigurieren und zu verwenden. Alle für die Bereitstellung der Aktivitätstypen erforderlichen Daten sind in einer XML-Datei enthalten. Um ein Beispiel für das XML-Dokument anzuzeigen, das einen Aktivitätstyp angibt, exportieren Sie ein Richtlinientypobjekt und betrachten dann die gespeicherte XML-Datei.

Gehen Sie folgendermaßen vor, um die exportierten Richtlinientypobjekte und Container zu importieren:

1. Klicken Sie in der Quest One ActiveRoles-Konsolenstruktur unter **Configuration/Server Configuration/Policy Types** mit der rechten Maustaste auf den Richtlinientypcontainer, in den Sie die exportierten Richtlinientypobjekte und Container importieren möchten.
2. Klicken Sie auf **Richtlinientypen importieren** und öffnen Sie dann die XML-Datei, die Sie importieren möchten.

Hierdurch werden neue Richtlinientypobjekte und Container im ausgewählten Container erstellt. Außerdem werden neue Skriptmodule im Container **Configuration/Script Modules** erstellt und mit den neu erstellten Richtlinientypobjekten verknüpft.

Konfigurieren einer Aktivität eines benutzerdefinierten Typs

Nach Bereitstellung eines benutzerdefinierten Aktivitätstyps kann ein Quest One ActiveRoles-Administrator eine Aktivität dieses Typs zu einem Workflow hinzufügen. Ziehen Sie hierzu den Aktivitätstyp auf das Arbeitsablaufprozessdiagramm in Workflow Designer.

Gehen Sie folgendermaßen vor, um eine Arbeitsablaufaktivität eines benutzerdefinierten Richtlinientyps zu konfigurieren:

1. Erweitern Sie in der Quest One ActiveRoles-Konsolenstruktur **Konfiguration | Richtlinien | Workflow** und wählen Sie den Workflow, in welchem Sie eine Aktivität hinzufügen möchten.

   Hierdurch wird das Workflow Designer-Fenster im Bereich „Details" geöffnet, das die Arbeitsablaufdefinition als ein Prozessdiagramm darstellt.

2. Ziehen Sie im Bereich „Details" den Aktivitätstyp vom linken Bereich auf das Prozessdiagramm.

   *Im Bereich links neben dem Workflow-Prozessdiagramm werden alle Aktivitätstypen, die in Ihrer Quest One ActiveRoles-Umgebung festgelegt sind, aufgeführt. Die integrierten Aktivitätstypen werden im Bereich **Standard** zusammen mit den benutzerdefinierten Aktivitätstypen, deren Richtlinientypobjekte sich direkt im Container **Policy Types** befinden, aufgelistet. Die anderen benutzerdefinierten Aktivitätstypen werden unter den Namen der Container aufgelistet, in denen sich die entsprechenden Richtlinientypobjekte befinden. Die Liste umfasst nur solche Container, die sich direkt im Container **Policy Types** befinden. Die Namen der dazwischen liegenden Container werden nicht angezeigt.*

3. Klicken Sie mit der rechten Maustaste auf den Namen der Aktivität, die Sie zum Prozessdiagramm hinzugefügt haben, und klicken Sie dann auf **Eigenschaften**.

4. Legen Sie auf der Seite **Eigenschaften**Parameterwerte für die Aktivität fest: Klicken Sie auf den Namen eines Parameters in der Liste und klicken Sie dann auf **Bearbeiten**.

   Parameter kontrollieren das Verhalten der Aktivität. Wenn Quest One ActiveRoles die Aktivität ausführt, werden die Parameterwerte zur Skriptfunktion weitergegeben. Die von der Skriptfunktion durchgeführten Vorgänge und die Ergebnisse dieser Vorgänge hängen von den Parameterwerten ab.

   *Durch Anklicken von **Bearbeiten** wird eine Seite angezeigt, auf der Sie einen oder mehrere Werte für den ausgewählten Parameter hinzufügen, entfernen oder auswählen können. Für jeden Parameter definiert das von der Aktivität verwendete Skript den Namen des Parameters und andere Merkmale wie etwa eine Beschreibung, eine Liste der möglichen Werte, den Standardwert und ob ein Wert erforderlich ist oder nicht. Wenn eine Liste der möglichen Werte definiert ist, dann können Sie nur Werte aus dieser Liste auswählen.*

5. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** zu schließen, und klicken Sie dann in Workflow Designer auf **Änderungen speichern**.

Löschen eines Richtlinientypobjekts

Sie können ein Richtlinientypobjekt löschen, wenn Sie keine Aktivitäten des von diesem Objekt definierten Typs mehr hinzufügen müssen.

Beachten Sie vor dem Löschen eines Richtlinientypobjekts die folgenden Hinweise:

- Sie können ein Richtlinientypobjekt nur dann löschen, wenn keine Aktivitäten des entsprechenden Typs in irgendeinem Arbeitsablauf vorhanden sind. Prüfen Sie jede Arbeitsablaufdefinition und entfernen Sie die Aktivitäten dieses Typs (falls vorhanden) aus dem Arbeitsablauf, bevor Sie das Richtlinientypobjekt löschen.
- Durch das Löschen eines Richtlinientypobjekts wird dieses dauerhaft aus der Quest One ActiveRoles-Datenbank gelöscht. Wenn Sie diesen Aktivitätstyp erneut verwenden möchten, sollten Sie das Richtlinientypobjekt in eine XML-Datei exportieren, bevor Sie das Objekt löschen.
- Durch das Löschen eines Richtlinientypobjekts wird das mit diesem Objekt verbundene Skriptmodul nicht gelöscht. Das Skriptmodul wird nicht gelöscht, da es möglicherweise von anderen Aktivitäten verwendet wird. Wenn das Skriptmodul nicht mehr benötigt wird, kann es separat gelöscht werden.

Gehen Sie folgendermaßen vor, um ein Richtlinientypobjekt zu löschen:

- Klicken Sie mit der rechten Maustaste auf das Richtlinientypobjekt in der Quest One ActiveRoles-Konsole und klicken Sie dann auf **Löschen**.

7

Temporare Gruppenmitgliedschaften

- Beschreibung von temporären Gruppenmitgliedschaften
- Verwenden von temporären Gruppenmitgliedschaften

Beschreibung von temporären Gruppenmitgliedschaften

Durch die Verwendung temporärer Gruppenzugehörigkeiten erteilt Quest One ActiveRoles die Fähigkeit, die Aufgaben, Gruppenmitglieder, die die Gruppenzugehörigkeit nur für eine bestimmte Zeitspanne brauchen, hinzuzufügen oder zu entfernen, zu automatisieren. Beim Hinzufügen von Objekten wie etwa Benutzern, Computern oder Gruppen zu einer bestimmten Gruppe kann ein Administrator festlegen, dass die Objekte zum gewählten Zeitpunkt zu der Gruppe hinzugefügt werden sollen. Außerdem kann er angeben, wann diese Objekte aus der Gruppe entfernt werden sollen.

Die Funktionalität der temporären Gruppenzugehörigkeit, die Quest One ActiveRoles bietet, kann Organisationen helfen, Gruppen effizient und für eine bestimmte Zeitspanne Benutzer und sonstige Objekte Gruppen zuzuweisen. Obwohl in vielen Fällen Objekte, die zu einer Gruppe hinzugefügt werden, auf unbestimmte Zeit Mitglieder der Gruppe bleiben, besteht in vielen Organisationen die Notwendigkeit der temporären Zuweisung von Objekten zu bestimmten Gruppen. Zu den typischen Szenarien gehört etwa die Gewährung des Zugriffs auf spezifische Ressourcen für die Dauer eines bestimmten Projekts oder die temporäre Zuweisung der Rolle als ein Serveradministrator.

Die Verwaltung temporärer Gruppenzuweisungen stellt hohe Herausforderungen für die Administratoren dar, da ein hohes Maß administrativer Überwachung erforderlich ist, um sicherzustellen, dass die Gruppenzuweisungen wirklich nur temporär sind und aufgrund mangelnder Kontrolle über Gruppenzugehörigkeiten nicht permanent werden. Quest One ActiveRoles erfüllt diese Anforderungen durch die Möglichkeit, Gruppenmitglieder automatisch und nach einem Zeitplan synchronisiert hinzuzufügen oder zu entfernen.

Die temporäre Gruppenmitgliedschaftsfunktionalität weitet die Vorteile von Quest One ActiveRoles auf folgende Bereiche aus:

- **Sicherheit.** Durch enge Kontrolle über Änderungen der Gruppenmitgliedschaften einschließlich richtlinienbasierter Regeln und Einschränkungen, Genehmigungsänderungen und Änderungsüberwachung reduziert Quest One ActiveRoles die Sicherheitsrisiken für Systeme, Anwendungen und Dienste, die Active-Directory-Gruppen für die Zugriffsgenehmigung verwenden. Das rechtzeitige Hinzufügen und Entfernen von Gruppenmitgliedern gewährleistet, dass die Benutzer nur für die erforderliche Dauer Zugriff auf System und Ressourcen haben. So werden die Möglichkeit und der Umfang des Zugriffs eingeschränkt.
- **Verfügbarkeit.** Durch die automatische Auffüllung von Gruppen auf der Grundlage konfigurierbarer Richtlinien macht Quest One ActiveRoles entsprechende Netzwerkressourcen für entsprechende Benutzer dann verfügbar, wenn sie auf diese Ressourcen zugreifen müssen. Die Möglichkeit, einen Zeitplan für das Hinzufügen und Entfernen von Gruppenmitgliedern zu erstellen, ist hilfreich in Situationen, in denen der temporäre Zugriff für eine relativ kurze Dauer erforderlich ist oder wenn kurzfristig zahlreiche Anforderungen zur Änderung der Gruppenmitgliedschaften eintreffen.
- **Verwaltbarkeit.** Quest One ActiveRoles beschleungt die Verwaltung, um Benutzer Gruppen zuzuordnen und Mitglieder aus Gruppen zu entfernen. Eine einheitliche und zuverlässige Kontrolle dieser Bereitstellung- und Deprovisionierungsaktivitäten verringert den Arbeitsaufwand für die Personen, die für die Verwaltung von Active Directory-Gruppen verantwortlich sind. Eine unbeaufsichtigte, auf einer Planung beruhende Handhabung der temporären Gruppenmitgliedschaften trägt zur Gewährleistung der Konformität mit Änderungs- und Zugriffsrichtlinien bei und vereinfacht gleichzeitig die Verwaltung von Gruppenmitgliedschafts-Änderungsanforderungen.

- **Kompatibilität.** Quest One ActiveRoles reduziert die Risiken der Einhaltung gesetzlicher Bestimmung durch Sicherstellung, dass geeignete und effiziente Kontrollen für die Gruppenzugehörigkeiten vorhanden sind. Da Active Directory-Gruppen verwendet werden, um den Zugriff auf Systeme, Anwendungen und Daten zu autorisieren, trägt die Kontrolle der Zuweisung von Benutzern zu Gruppen auf einer temporären Basis dazu bei, dass die Organisationen die Anforderungen im Hinblick auf die Trennung von Pflichten und den Datenschutz erfüllen.

Quest One ActiveRoles stellt die temporäre Gruppenzugehörigkeitsfunktionalität für die Active-Directory-Domänendienste (AD DS) und die Active Directory Lightweight Services (AD LDS) zur Verfügung.

Die Funktion der temporären Gruppenmitgliedschaft automatisiert die Aufgaben des Hinzufügens und Entfernens von Benutzern zu bzw. aus Gruppen in Situationen, in denen die Benutzer die Gruppenmitgliedschaft nur für einen bestimmten Zeitraum benötigen. Durch Anwendung von Einstellungen für die temporäre Gruppenmitgliedschaft können die Administratoren die Zuweisung von ausgewählten Objekten zu einer bestimmten Gruppe planen und angeben, wann die Objekte aus der Gruppe entfernt werden sollen.

Die von Quest One ActiveRoles zur Verfügung gestellten Hauptfunktionen für die Verwaltung temporärer Gruppenzugehörigkeiten lauten wie folgt:

- **Temporäre Gruppenmitglieder hinzufügen.** Die Benutzerschnittstelle für die Auswahl von Objekten in der Quest One ActiveRoles-Konsole und an der Webschnittstelle stellt zahlreiche Optionen bereit, um festzulegen, wann die ausgewählten Objekte zu der gewählten Gruppe hinzugefügt und wann die ausgewählten Objekte aus der Gruppe entfernt werden sollen. Es ist möglich, die Objekte sofort zur Gruppe hinzuzufügen und anzugeben, dass die Objekte nicht aus der Gruppe entfernt werden sollen.
- **Temporäre Mitglieder einer Gruppe anzeigen.** Die Liste der Gruppenmitglieder (die **Mitglieder**seite), die von der Quest One ActiveRoles-Konsole oder der Webschnittstelle angezeigt wird, macht es möglich, zwischen normalen und temporären Gruppenmitgliedern zu unterscheiden. Es ist auch möglich, die temporären Mitglieder, die laut Planung zukünftig zur Gruppe hinzugefügt werden sollen, jedoch aktuell noch keine Mitglieder der Gruppe sind, auszublenden oder anzuzeigen.
- **Temporäre Mitgliedschaft eines Objekts anzeigen.** Die Liste der Gruppenmitgliedschaften für ein bestimmtes Objekt (die **Seite Mitglied von**) ermöglicht die Unterscheidung zwischen den Gruppen, in denen das Objekt ein normales Mitglied ist, und den Gruppen, in denen das Objekt ein temporäres Mitglied ist. Es ist auch möglich, die Gruppen auszublenden oder anzuzeigen, in die das Objekt laut Planung zukünftig hinzugefügt werden soll.
- **Temporäre Gruppenmitgliedschaften neu planen.** Sowohl die Seite **Mitglieder** als auch die Seite **Mitglied von** bieten die Möglichkeit, die Einstellungen für die temporäre Gruppenmitgliedschaft anzuzeigen oder zu ändern. Auf der Seite **Mitglieder** für eine bestimmte Gruppe können Sie ein Mitglied auswählen und das Datum und die Uhrzeit, wann das Mitglied zur Gruppe hinzugefügt bzw. aus ihr entfernt werden soll, anzeigen oder ändern. Auf der Seite **Mitglied von** für ein bestimmtes Objekt können Sie eine Gruppe auswählen und das Datum und die Uhrzeit, wann das Objekt zur Gruppe hinzugefügt bzw. aus ihr entfernt werden soll, anzeigen oder ändern.
- **Temporäres Mitglied zu permanentem Mitglied machen.** Die Einstellungen für die temporäre Gruppenmitgliedschaft bieten die Möglichkeit, anzugeben, dass das Objekt nicht aus der Gruppe entfernt werden soll und somit ein temporäres Mitglied zu einem permanenten Mitglied zu machen. Wenn die Einstellungen für die temporäre Gruppenmitgliedschaft für ein

bestimmtes Objekt so konfiguriert sind, dass ein Objekt sofort zu einer bestimmten Gruppe hinzugefügt und nie aus der Gruppe entfernt wird, dann wird das Objekt zu einem normalen Mitglied dieser Gruppe. Entsprechend wird ein normales Mitglied, wenn andere Einstellungen für die temporäre Gruppenmitgliedschaft angegeben werden, in ein temporäres Mitglied konvertiert.

- **Temporäre Gruppenmitglieder entfernen.** Sowohl die Seite **Mitglieder** als auch die Seite **Mitglied von** bietet die Funktion zum Entfernen von Gruppenmitgliedschaften (temporär oder normal). Wenn Sie die Funktion „Entfernen" auf temporäre Mitglieder einer Gruppe anwenden, dann werden die Mitglieder zusammen mit allen Einstellungen für die temporäre Gruppenmitgliedschaft, die für diese Mitglieder gelten, entfernt. Gleiches gilt, wenn Sie die Funktion „Entfernen" auf Gruppen anwenden, in denen ein bestimmtes Objekt ein temporäres Mitglied ist.

Durch die temporäre Gruppenzugehörigkeitsfunktionalität stellt Quest One ActiveRoles sicher, dass die Benutzer Gruppenzugehörigkeiten nur für den benötigten Zeitraum haben, indem die temporäre Art der Gruppenzugehörigkeiten bei Bedarf erzwungen wird und das Risiko, dass Gruppenzugehörigkeiten länger dauern als notwendig, beseitigt wird.

Verwenden von temporären Gruppenmitgliedschaften

Durch die Verwendung von temporären Gruppenmitgliedschaften können Sie Gruppenmitgliedschaften von Objekten wie etwa Benutzer- oder Computerkonten verwalten, die nur für einen bestimmten Zeitraum Mitglieder von bestimmten Gruppen sein müssen. Diese Funktion von Quest One ActiveRoles bietet Ihnen Flexibilität hinsichtlich der Entscheidung, welche Objekte wie lange Gruppenmitgliedschaften erfordern. Außerdem ermöglicht sie eine einfache Verfolgung dieser Objekte.

Dieser Abschnitt begleitet Sie durch die Aufgaben, temporäre Gruppenzugehörigkeiten in der Quest One ActiveRoles-Konsole zu verwalten. Wenn Sie zur Anzeige und Änderung von Gruppenmitgliedschaftslisten berechtigt sind, dann können Sie temporäre Gruppenmitglieder hinzufügen, anzeigen und entfernen sowie Einstellungen für die temporäre Gruppenmitgliedschaft von Gruppenmitgliedern anzeigen und bearbeiten.

Hinzufügen von temporären Mitgliedern

Ein temporäres Mitglied einer Gruppe ist ein Objekt wie etwa ein Benutzer, ein Computer oder eine Gruppe, das für das Hinzufügen zur Gruppe bzw. zum Löschen aus der Gruppe geplant ist. Sie können temporäre Mitglieder mit Hilfe der Quest One ActiveRoles-Konsole hinzufügen und konfigurieren.

Gehen Sie folgendermaßen vor, um temporäre Mitglieder zu einer Gruppe hinzuzufügen:

1. Klicken Sie in der Quest One ActiveRoles-Konsole mit der rechten Maustaste auf die Gruppe und dann auf **Eigenschaften**.
2. Klicken Sie auf der Registerkarte **Mitglieder** im Dialogfeld **Eigenschaften** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Objekte auswählen** auf **Einstellungen für die temporäre Gruppenmitgliedschaft**.
4. Wählen Sie im Dialogfeld **Einstellungen für die temporäre Gruppenmitgliedschaft** die entsprechenden Optionen und klicken Sie dann auf **OK**:
   - Um die temporären Mitglieder an einem bestimmten Datum in der Zukunft zur Gruppe hinzuzufügen, wählen Sie **An diesem Datum**unter **Zur Gruppe hinzufügen** und anschließend das gewünschte Datum und die gewünschte Uhrzeit aus.
   - Um die temporären Mitglieder sofort zur Gruppe hinzuzufügen, wählen Sie **Jetzt** unter **Zur Gruppe hinzufügen**.
   - Um die temporären Mitglieder an einem bestimmten Datum in der Zukunft aus der Gruppe zu entfernen, wählen Sie **An diesem Datum** unter **Aus der Gruppe entfernen** und anschließend das gewünschte Datum und die gewünschte Uhrzeit aus.
   - Um die temporären Mitglieder auf unbestimmte Zeit in der Gruppe zu behalten, wählen Sie **Nie** unter **Aus der Gruppe entfernen**.
5. Geben Sie im Dialogfeld **Objekte auswählen** die Namen der Objekte ein, die Sie zu temporären Mitgliedern der Gruppe machen möchten, oder wählen Sie sie aus und klicken Sie dann auf **OK**.

6. Klicken Sie auf **Anwenden** im Dialogfeld **Eigenschaften** für die Gruppe.

- Um temporäre Mitglieder einer Gruppe hinzuzufügen, müssen Sie befugt sein, Mitglieder zur Gruppe hinzuzufügen bzw. aus ihr zu entfernen. Die entsprechende Befugnis kann durch Anwenden der Zugriffsvorlage **Groups - Add/Remove Members** delegiert werden.
- Sie können ein Objekt zu einem temporären Mitglied von bestimmten Gruppen machen, indem Sie die Objekteigenschaften anstelle der Gruppeneigenschaften verwalten. Öffnen Sie das Dialogfeld **Eigenschafte** für dieses Objekt und klicken Sie dann auf der Registerkarte **Mitglied von** auf **Hinzufügen**. Geben Sie im Dialogfeld **Objekte auswählen** die Einstellungen für die temporäre Gruppenmitgliedschaft an und geben Sie dann die Namen der Gruppen abhängig von Ihrer Situation an.

Anzeigen von temporären Mitgliedern

Die von der Quest One ActiveRoles-Konsole angezeigte Liste der Gruppenmitglieder ermöglicht es, zwischen normalen und temporären Gruppenmitgliedern zu unterscheiden. Es ist auch möglich, so genannte *ausstehende Mitglieder* auszublenden oder anzuzeigen. Dies sind die temporären Mitglieder, die laut Planung zukünftig zur Gruppe hinzugefügt werden sollen, jedoch aktuell noch keine Mitglieder der Gruppe sind.

Gehen Sie folgendermaßen vor, um temporäre Mitglieder einer Gruppe anzuzeigen:

1. Klicken Sie in der Quest One ActiveRoles-Konsole mit der rechten Maustaste auf die Gruppe und dann auf **Eigenschaften**.
2. Untersuchen Sie die Liste auf der Registerkarte **Mitglieder** im Dialogfeld **Eigenschaften**:
   - Ein kleines Uhrsymbol wird über dem Symbol für die temporären Mitglieder angezeigt.
   - Wenn das Kontrollkästchen **Ausstehende Mitglieder anzeigen** aktiviert ist, enthält die Liste auch die temporären Mitglieder, die noch nicht zur Liste hinzugefügt wurden. Symbole, die solche Mitglieder angeben, werden orange angezeigt.

Die Liste der Gruppenmitgliedschaften für ein bestimmtes Objekt ermöglicht die Unterscheidung zwischen den Gruppen, in denen das Objekt ein normales Mitglied ist, und den Gruppen, in denen das Objekt ein temporäres Mitglied ist. Es ist auch möglich, so genannte *ausstehende Gruppenmitgliedschaften* auszublenden oder anzuzeigen. Ausstehende Gruppenmitgliedschaften sind die Gruppen, in die das Objekt laut Planung zukünftig hinzugefügt werden soll.

Gehen Sie folgendermaßen vor, um die Gruppen anzuzeigen, in denen ein Objekt ein temporäres Mitglied ist:

1. Klicken Sie in der Quest One ActiveRoles-Konsole mit der rechten Maustaste auf das Objekt und dann auf **Eigenschaften**.
2. Untersuchen Sie die Liste auf der Registerkarte **Mitglied von** im Dialogfeld **Eigenschaften**:
   - Ein kleines Uhrsymbol wird über dem Symbol für die Gruppen angezeigt, in denen das Objekt ein temporäres Mitglied ist.
   - Wenn das Kontrollkästchen **Ausstehende Gruppenmitgliedschaften anzeigen** aktiviert ist, enthält die Liste auch die Gruppen, zu denen das Objekt laut Planung zukünftig hinzugefügt werden soll. Symbole, die solche Gruppen angeben, werden orange angezeigt.

Neuplanen von temporären Gruppenmitgliedschaften

Die Einstellungen für die temporäre Gruppenmitgliedschaft für ein Gruppenmitglied umfassen die Einstellungen *Startzeit* und *Endzeit*.

Die Startzeit gibt an, wann das Objekt zur Gruppe hinzugefügt wird. Hierbei kann es sich um ein bestimmtes Datum und eine bestimmte Uhrzeit oder um eine Angabe, dass das Objekt sofort zur Gruppe hinzugefügt werden soll, handeln.

Die Endzeit gibt an, wann das Objekt aus der Gruppe entfernt werden soll. Hierbei kann es sich um ein bestimmtes Datum und eine bestimmte Uhrzeit oder um eine Angabe, dass das Objekt nicht aus der Gruppe entfernt werden soll, handeln.

Sie können die Anfangs- und die Endzeiteinstellungen mit Hilfe der Quest One ActiveRoles-Konsole einsehen oder ändern.

Gehen Sie folgendermaßen vor, um die Start- oder Endzeit für ein Mitglied einer Gruppe anzuzeigen oder zu ändern:

1. Klicken Sie in der Quest One ActiveRoles-Konsole mit der rechten Maustaste auf die Gruppe und dann auf **Eigenschaften**.
2. Klicken Sie in der Liste auf der Registerkarte **Mitglieder** im Dialogfeld **Eigenschaften** auf das Mitglied und klicken Sie dann auf die Schaltfläche **Einstellungen für die temporäre Gruppenmitgliedschaft**.
3. Verwenden Sie das Dialogfeld **Einstellungen für die temporäre Gruppenmitgliedschaft**, um die Start- oder Endzeit anzuzeigen oder zu ändern.

Das Dialogfeld **Einstellungen für die temporäre Gruppenmitgliedschaft** umfasst die folgenden Optionen:

- **Zur Gruppe hinzufügen | Jetzt.** Gibt an, dass das Objekt sofort zur Gruppe hinzugefügt werden soll.
- **Zur Gruppe hinzufügen | An diesem Datum.** Gibt das Datum und die Uhrzeit an, an dem bzw. zu der das Objekt zur Gruppe hinzugefügt werden soll.
- **Aus der Gruppe entfernen | Nie.** Gibt an, dass das Objekt nicht aus der Gruppe entfernt werden soll.
- **Aus der Gruppe entfernen | An diesem Datum.** Gibt das Datum und die Uhrzeit an, an dem bzw. zu der das Objekt aus der Gruppe entfernt werden soll.

Für die normalen Mitglieder sind die Optionen **Zur Gruppe hinzufügen** und **Aus Gruppe entfernen** auf **Bereits hinzugefügt** bzw. **Nie** gesetzt. Sie können ein bestimmtes Datum für jede dieser Optionen festlegen, um ein normales Mitglied in ein temporäres Mitglied umzuwandeln.

- Sie können die Start- und Endzeiteinstellungen anzeigen und ändern, indem Sie ein Objekt anstelle der Gruppen, in denen das Objekt Mitglied ist, verwalten. Öffnen Sie das Dialogfeld **Eigenschaften** für dieses Objekt und wählen Sie dann auf der Registerkarte **Mitglied von** die Gruppe aus, für die Sie die Start- oder Endzeiteinstellungen des Objekts verwalten möchten, und klicken Sie dann auf **Einstellungen für die temporäre Gruppenmitgliedschaft**.

- Auf der Registerkarte **Mitglieder** oder **Mitglied von** können Sie die Start- oder Endzeiteinstellungen für mehrere Mitglieder oder Gruppen gleichzeitig ändern. Wählen Sie in der Liste auf der Registerkarte zwei oder mehr Elemente aus und klicken Sie dann auf **Einstellungen für die temporäre Gruppenmitgliedschaft**. Aktivieren Sie dann im Dialogfeld **Einstellungen für die temporäre Gruppenmitgliedschaft** die entsprechenden Kontrollkästchen, um die zu ändernden Einstellungen anzugeben, und nehmen Sie dann die gewünschten Änderungen vor.

Entfernen von temporären Mitgliedern

Sie können temporäre Gruppenmitglieder auf die gleiche Weise entfernen wie normale Gruppenmitglieder. Durch das Entfernen eines temporären Mitglieds aus einer Gruppe werden die Einstellungen für die temporäre Gruppenmitgliedschaft für dieses Objekt in Hinblick auf diese Gruppe gelöscht. Folglich wird das Objekt nicht zur Gruppe hinzugefügt. Wenn das Objekt zum Zeitpunkt des Entfernens bereits zu der Gruppe gehört, dann wird es aus der Gruppe entfernt.

Gehen Sie folgendermaßen vor, um ein temporäres Mitglied aus einer Gruppe zu entfernen:

1. Klicken Sie in der Quest One ActiveRoles-Konsole mit der rechten Maustaste auf die Gruppe und dann auf **Eigenschaften**.
2. Klicken Sie auf der Registerkarte **Mitglieder** im Dialogfeld **Eigenschaften** auf das Mitglied, klicken Sie dann auf **Entfernen** und klicken Sie anschließend auf **Anwenden**.

Sie können ein Objekt, das ein temporäres Mitglied einer Gruppe ist, entfernen, indem Sie das Objekt anstelle der Gruppe verwalten. Öffnen Sie das Dialogfeld **Eigenschaften** für dieses Objekt und wählen Sie dann auf der Registerkarte **Mitglied von** die Gruppe aus der Liste aus und klicken Sie dann auf **Entfernen**.

8

Gruppenfamilie

- Grundlegendes zu Gruppenfamilien
- Erstellen einer Gruppenfamilie
- Verwalten einer Gruppenfamilie
- Szenario: Abteilungsbezogene Gruppenfamilie

Grundlegendes zu Gruppenfamilien

Quest One ActiveRoles stellt eine separate Kategorie regelorientierter Richtlinien speziell für die automatische Gruppenbereitstellung (AutoProvisioning für Gruppen) bereit. Jede Richtlinie dieser Kategorie, die als *Gruppenfamilie* bezeichnet wird, dient als Kontrollmechanismus für die Erstellung und Auffüllung von Gruppen.

Die Gruppenfamilie erstellt automatisch Gruppen und pflegt Gruppenmitgliedschaftslisten. Dabei hält sie konfigurierbare Regeln ein. Die Gruppenmitgliedschaft kann somit anhand von Objekteigenschaften im Verzeichnis definiert werden. Die Gruppenfamilie ermöglicht außerdem das Erstellen neuer Gruppen anhand neuer Werte, die in Objekteigenschaften erkannt werden.

Wenn Sie beispielsweise Gruppen anhand des geografischen Standorts verwalten möchten, können Sie eine Gruppenfamilie konfigurieren, die Gruppen für jeden Wert in der Eigenschaft „Stadt" von Benutzerkonten erstellt und pflegt. Die Gruppenfamilie erkennt alle Werte dieser Eigenschaft im Verzeichnis und generiert für jeden Wert eine Gruppe. Diese wird mit den Benutzern aufgefüllt, die denselben Wert für die Eigenschaft „Stadt" aufweisen. Wenn der Eigenschaft „Stadt" für einige Benutzer ein neuer Wert zugewiesen wird, erstellt die Gruppenfamilie automatisch eine neue Gruppe für diese Benutzer. Wenn für einen Benutzer der Wert der Eigenschaft „Stadt" geändert wird, ändert die Gruppenfamilie die Gruppenmitgliedschaft für diesen Benutzer entsprechend.

Die Konfiguration einer Gruppenfamilie muss nicht auf eine einzelne Objekteigenschaft beschränkt sein. Sie kann aus so vielen Eigenschaften kombiniert werden wie nötig. Beispielsweise kann eine Gruppenfamilie so eingerichtet werden, dass sie die Eigenschaften für die Abteilung und die Stadt berücksichtigt. Folglich erstellt und pflegt die Gruppenfamilie eine separate Gruppe für jede Abteilung an jedem geografischen Standort.

Entwurfsübersicht

Die wichtigsten Entwurfselemente der Gruppenfamilie sind Folgende:

- **Bereichsdefinierung nach Objektspeicherort.** Bestimmt die Verzeichniscontainer, die die von der Gruppenfamilie zu verwaltenden Objekte enthalten. Der Bereich der Gruppenfamilie kann auf bestimmte Container eingeschränkt werden, sodass sie sich nur auf die Objekte in diesen Containern auswirkt.
- **Bereichsdefinierung nach Objekttyp und Eigenschaft.** Bestimmt den Typ der Objekte, z.B. „Benutzer" oder „Computer", die von der Gruppenfamilie verwaltet werden sollen. Der Bereich der Gruppenfamilie kann so auf eine Gruppe von Objekten eines bestimmten Typs beschränkt werden. Um den Bereich weiter zu verfeinern, können Sie einen Filter anwenden, mit dem die Gruppenfamilie nur die Objekte verwaltet, die bestimmte Bedingungen in Bezug auf Eigenschaften erfüllen.
- **Gruppierung nach Objekteigenschaft.** Die Gruppenfamilie teilt die verwalteten Objekte (den Bereich) in *Gruppierungen* ein. Jede Gruppierung besteht aus den Objekten, bei denen die angegebenen Eigenschaften (die so genannten *Gruppieren-nach-Eigenschaften*) die gleiche Kombination von Werten aufweisen. Wenn beispielsweise die Abteilungseigenschaft als Gruppieren-nach-Eigenschaft für Benutzerobjekte angegeben ist, enthält jede Gruppierung nur die Benutzer aus einer bestimmten Abteilung.
- **Erstellen oder Erfassung von Gruppen.** Normalerweise erstellt die Gruppenfamilie für jede Gruppierung eine neue Gruppe, um sie der Gruppierung zuzuordnen (mit ihr zu verknüpfen). Dabei wird sichergestellt, dass nur Mitglieder dieser Gruppierung in der Gruppe enthalten sind. Beim Erstellen von Gruppen für Gruppierungen verwendet die Gruppenfamilie Gruppenbenennungsregeln, die auf den Werten der Gruppieren-nach-Eigenschaften basieren. Eine weitere Option ist die manuelle Verknüpfung vorhandener Gruppen mit Gruppierungen; dieser Vorgang wird als *Erfassen von Gruppen* bezeichnet.

- **Beibehalten von Gruppenmitgliedschaftslisten auf der Grundlage von Gruppierungen.** Während jeder folgenden Ausführung der Gruppenfamilie werden die Gruppierungen neu berechnet, und die zugehörigen Gruppen werden anhand der Änderungen in den Gruppierungen aktualisiert. Mit diesem Vorgang wird sichergestellt, das die Gruppe, die der jeweiligen Gruppierung zugeordnet ist, genau dieselben Objekte enthält wie die Gruppierung. Wenn eine neue Gruppierung gefunden wird, erstellt die Gruppenfamilie eine Gruppe, verknüpft die Gruppe mit der neuen Gruppierung, und füllt die Mitgliedschaftsliste der Gruppe mit den Objekten dieser Gruppierung auf.
- **Anpassen der Eigenschaften von generierten Gruppen.** Wenn die Gruppenfamilie eine neue Gruppe für eine Gruppierung erstellt, werden der Name und andere Eigenschaften der neuen Gruppe anhand der Regeln angepasst, die in der Gruppenfamilienkonfiguration definiert sind. Mit diesen Regeln wird außerdem Folgendes bestimmt: der Container, in dem neue Gruppen erstellt werden sollen, die Einstellungen für Gruppentyp und Bereich sowie Einstellungen im Zusammenhang mit Exchange, z.B. die Frage, ob die generierten Gruppen E-Mail-fähig sein sollen.
- **Ausführen auf einer geplanten Basis.** Die Gruppenfamilie ist eine zustandsbasierte Richtlinie. Bei jeder Ausführung analysiert sie den Zustand der Verzeichnisdaten und führt anhand der Analyseergebnisse bestimmte Bereitstellungsaktionen aus. Die Gruppenfamilie kann für die Ausführung in regelmäßigen Intervallen geplant werden. Dabei wird sichergestellt, dass alle notwendigen Gruppen vorhanden sind und dass die Gruppenmitgliedschaftslisten aktuell und richtig sind. Außerdem kann die Gruppenfamilie jederzeit manuell ausgeführt werden.
- **Vorgangsübersicht-Protokoll.** Quest One ActiveRoles stellt ein Protokoll mit Zusammenfassungsinformationen zur letzten Ausführung der Gruppenfamilie bereit. Das Protokoll enthält ggf. Beschreibungen der Fehlersituationen, die während der Ausführung aufgetreten sind, und fasst die quantitativen Ergebnisse der Ausführung zusammen, z.B. die Anzahl aktualisierter Gruppen, die Anzahl erstellter Gruppen und die Anzahl der Objekte, deren Gruppenmitgliedschaften geändert wurden.

Funktionsweise

Die Gruppenfamilienkonfiguration gibt Regeln an, mit denen Folgendes bestimmt wird:

- **Bereich.** Die von der Gruppenfamilie verwalteten Verzeichnisobjekte werden als der *Bereich* bezeichnet. Der Bereich kann auf Objekte einer bestimmten Kategorie (wie z.B. Benutzerobjekte) eingeschränkt werden, die sich in bestimmten Organisationseinheiten befinden. Außerdem kann der Bereich durch Filterung weiter verfeinert werden.
- **Gruppierungen.** Die Gruppenfamilie teilt den Bereich in Teilmengen auf, die als *Gruppierungen* bezeichnet werden. Jede Gruppierung besteht aus Objekten, die für bestimmte Eigenschaften die gleichen Werte aufweisen. Diese Eigenschaften werden als *Gruppieren-nach-Eigenschaften* bezeichnet. Eine Gruppierung wir also durch eine bestimmte Kombination von Werten der Gruppieren-nach-Eigenschaften identifiziert. Die Liste aller dieser Kombinationen wird als Teil der Gruppenfamilienkonfiguration gespeichert und gepflegt.
- **Gruppennamen.** Falls nichts anderes angegeben ist, erstellt die Gruppenfamilie für jede gefundene neue Gruppierung eine neue Gruppe. Der Gruppenname wird anhand der Benennungsregeln für Gruppen generiert. Sie können auch vorhandene Gruppen manuell zu einigen Gruppierungen zuweisen. Dann *erfasst* die Gruppenfamilie diese Gruppen.
- **Verknüpfungen.** Für jede Gruppierung erstellt oder erfasst die Gruppenfamilie eine Gruppe, verknüpft sie mit der Gruppierung und füllt sie mit den Objekten der Gruppierung auf. Während jeder folgenden Ausführung verwendet die Gruppenfamilie die Verknüpfungsinformationen, um die Gruppe zu erkennen, die mit der Gruppierung verknüpft ist, und aktualisiert die Mitgliedschaftsliste dieser Gruppe anhand der Änderungen in der Gruppierung. Die Gruppen, deren Informationen der Gruppenfamilie über die Verknüpfungen zur Verfügung stehen, werden als *kontrollierte Gruppen* bezeichnet.

Während der ersten Ausführung führt die Gruppenfamilie also Folgendes aus:

1. Der Bereich wird berechnet und analysiert, um eine Liste aller vorhandenen Wertekombinationen der Gruppieren-nach-Eigenschaften zu erstellen. Die Liste wird dann der Gruppenfamilienkonfiguration hinzugefügt.
2. Für jede Kombination von Werten wird eine Gruppierung berechnet, die aus allen Objekten im Bereich besteht, deren Gruppieren-nach-Eigenschaften auf die aus dieser Kombination abgeleiteten Werte festgelegt sind.
3. Für jede Gruppierung wird eine Gruppe erstellt oder erfasst und mit der Gruppierung verknüpft. Die Gruppenfamilienkonfiguration wird mit Informationen zu diesen Verknüpfungen aktualisiert. Die Gruppenfamilienkonfiguration bestimmt, ob eine Gruppe erstellt oder erfasst werden soll.
4. Für jede Gruppe, die mit einer bestimmten Gruppierung (kontrollierten Gruppe) verknüpft ist, wird die Mitgliedschaftsliste so aktualisiert, dass sie nur die Objekte dieser Gruppierung enthält. Alle vorhandenen Mitglieder werden aus der Gruppe entfernt. Dann werden alle in der Gruppierung gefundenen Objekte der Gruppe hinzugefügt.

Während einer weiteren Ausführung führt die Gruppenfamilie Folgendes aus:

1. Der Bereich wird berechnet und analysiert, um eine Liste aller vorhandenen Wertekombinationen der Gruppieren-nach-Eigenschaften zu erstellen. Die Gruppenfamilienkonfiguration wird dann anhand dieser Liste aktualisiert.
2. Für jede Kombination von Werten wird eine Gruppierung berechnet, die aus allen Objekten im Bereich besteht, deren Gruppieren-nach-Eigenschaften auf die aus dieser Kombination abgeleiteten Werte festgelegt sind.
3. Für jede Gruppierung wird eine Suche ausgeführt, die auf Verknüpfungsinformationen basiert, um die mit dieser Gruppierung verknüpfte Gruppe zu erkennen. Wenn die Gruppe gefunden wurde, wird ihre Mitgliedschaftsliste so aktualisiert, dass die Gruppe nur die in der Gruppierung gefundenen Objekte enthält. Andernfalls wird eine Gruppe erstellt oder erfasst, mit der Gruppierung verknüpft und mit den in der Gruppierung gefundenen Objekten aufgefüllt.

Beim Erstellen einer Gruppe für eine bestimmte Gruppierung generiert die Gruppenfamilie den Gruppennamen anhand der Benennungsregeln für Gruppen. Die Regeln definieren einen Namen, der auf der Wertekombination der Gruppieren-nach-Eigenschaften basiert, die die Gruppierung identifiziert. Die Benennungsregeln für Gruppen sind Teil der Gruppenfamilienkonfiguration.

Bei der Erfassung einer vorhandenen Gruppe für eine bestimmte Gruppierung verwendet die Gruppenfamilie eine Verknüpfung zwischen Gruppe und Gruppierung, die manuell erstellt und als Teil der Gruppenfamilienkonfiguration gespeichert wird. Die Verknüpfung gibt die Wertekombination der Gruppieren-nach-Eigenschaften an, um die Gruppierung zu identifizieren, und bestimmt die Gruppe, die mit dieser Gruppierung verknüpft werden soll.

Beim Füllen einer Gruppe verarbeitet die Gruppenfamilie nur die Objekte, die aus derselben Active Directory-Domäne wie die Gruppe selbst stammen. Wenn sich ein bestimmtes Objekt (wie etwa ein Benutzerkonto) in einer anderen Domäne befindet, kann die Gruppenfamilie das Objekt selbst dann nicht zur Gruppe hinzufügen, wenn dies von der Gruppenfamilie gemäß ihrer Konfiguration erwartet wird. Diese Einschränkung ist Absicht.

Erstellen einer Gruppenfamilie

Die Erstellung einer Gruppenfamilie besteht aus den folgenden zwei Schritten:

1. Erstellen der Gruppenfamilienkonfiguration
2. Ausführen der Gruppenfamilie zur Erstellung oder Erfassung von Gruppen

Die Quest One ActiveRoles-Konsole enthält den Assistenten „Neue Gruppenfamilie", mit dem Sie die Gruppenfamilienkonfiguration erstellen können. Der Assistent erstellt eine Gruppe, die als *Konfigurationsspeichergruppe* bezeichnet wird, und füllt sie mit den von Ihnen angegebenen Konfigurationsdaten auf.

Sie können beliebig viele Gruppenfamilien erstellen. Dabei steuert jede Gruppenfamilie eine bestimmte Sammlung von Gruppen. Wenn Sie eine Gruppe mit einer Gruppierung verknüpfen, stellt das Gruppenfamilienmodul sicher, dass die Gruppe nur von der Gruppenfamilie kontrolliert wird, die die Verknüpfung erstellt hat. So werden Konflikte vermieden.

Starten des Assistent für neue Gruppenfamilie

Sie können den Assistenten „Neue Gruppenfamilie" über die Quest One ActiveRoles-Konsole starten. Verwenden Sie dazu den Befehl **Neu | Gruppenfamilie** für die Organisationseinheit, in die Sie die Konfigurationsspeichergruppe platzieren möchten.

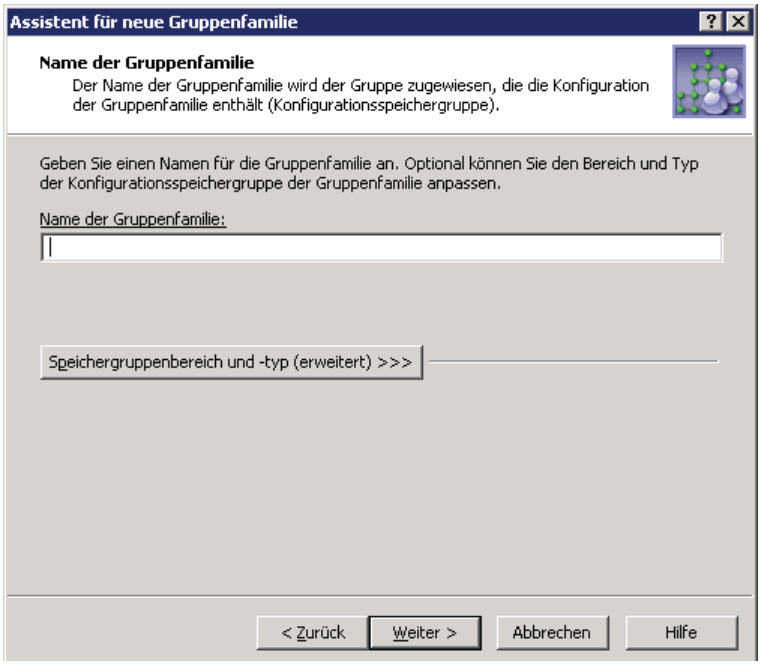
Gehen Sie folgendermaßen vor, um den Assistenten „Neue Gruppenfamilie" zu starten:

- Klicken Sie mit der rechten Maustaste auf die Organisationseinheit, die die Konfigurationsspeichergruppe der Gruppenfamilie enthalten soll, und wählen Sie **Neu | Gruppenfamilie** aus.

Name der Gruppenfamilie

Auf der ersten Seite nach der Willkommensseite stellen Sie einen Namen für die neue Gruppenfamilie bereit. Der Name wird der Gruppe zugewiesen, in der die Konfigurationsdaten der Gruppenfamilie gespeichert werden (der Konfigurationsspeichergruppe).

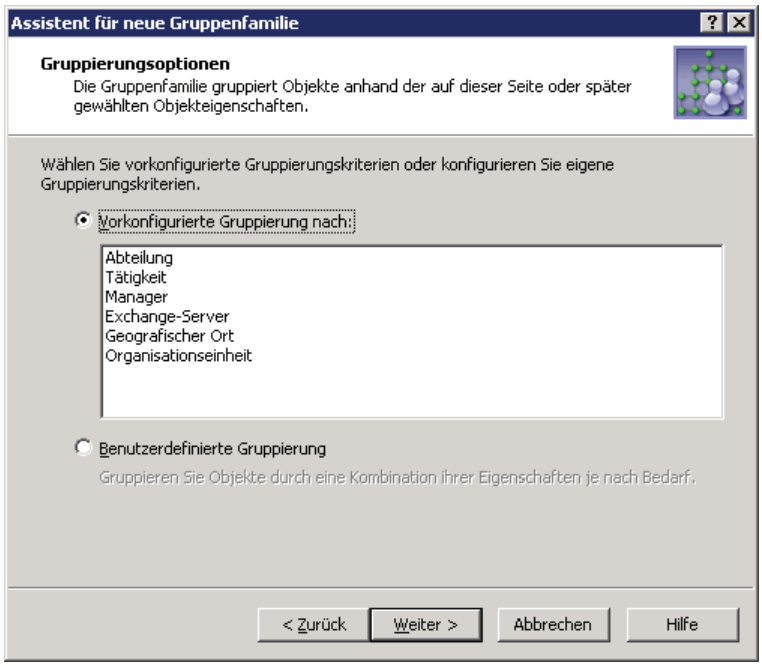
Außerdem können Sie auf dieser Seite den Typ und den Bereich der Konfigurationsspeichergruppe anpassen. Standardmäßig sind diese auf den Sicherheitstyp und den globalen Bereich festgelegt. Normalerweise müssen sie nicht geändert werden.


Assistent für neue Gruppenfamilie
Name der Gruppenfamilie
Der Name der Gruppenfamilie wird der Gruppe zugewiesen, die die Konfiguration der Gruppenfamilie enthält (Konfigurationsspeichergruppe).
Geben Sie einen Namen für die Gruppenfamilie an. Optional können Sie den Bereich und Typ der Konfigurationsspeichergruppe der Gruppenfamilie anpassen.
Name der Gruppenfamilie:
Speichergruppenbereich und -typ (erweitert) >>>
< Zurück
Weiter >
Abbrechen
Hilfe

Geben Sie einen Gruppenfamiliennamen ein und klicken Sie dann auf **Weiter**, um den Vorgang fortzusetzen.

Gruppierungsoptionen

Auf der nächsten Seite wird eine Liste häufig verwendeter Gruppierungskriterien bereitgestellt. Die Gruppenfamilie erstellt Gruppierungen anhand der Eigenschaften, die Sie auf dieser Seite auswählen können (Sie können sie aber auch später angeben).

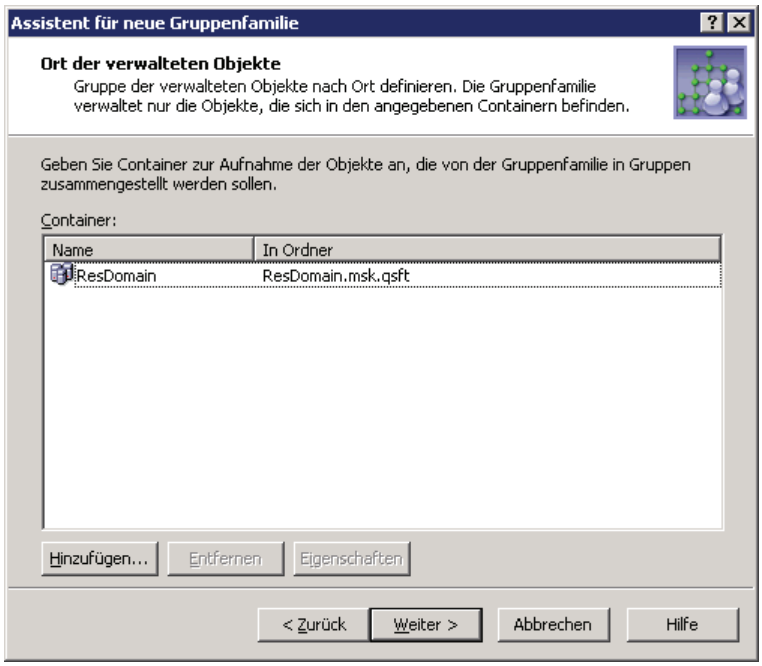


Sie können eine der folgenden Optionen auswählen:

- **Vorkonfigurierte Gruppierung.** Stellt eine Liste der häufig verwendeten Gruppieren-nach-Eigenschaften bereit. Dazu gehören die Abteilung, der Titel und der geografische Standort. Wählen Sie in der Liste einen Eintrag aus, um die Gruppieren-nach-Eigenschaften anzugeben. Später können Sie auf der Seite **Gruppieren-nach-Eigenschaften** des Assistenten die Liste der ausgewählten Gruppieren-nach-Eigenschaften anzeigen oder ändern.
- **Benutzerdefinierte Gruppierung.** Ermöglicht das Fortsetzen des Vorgangs ohne sofortiges Auswählen von Gruppieren-nach-Eigenschaften. Der Assistent fordert Sie später auf der Seite **Gruppieren-nach-Eigenschaften** zum Festlegen einer Liste von Gruppieren-nach-Eigenschaften auf.

Ort der verwalteten Objekte

Auf der nächsten Seite werden Sie aufgefordert, die Verzeichniscontainer anzugeben, die die von dieser Gruppenfamilie zu verwaltenden Objekte enthalten. Der Bereich der Gruppenfamilie kann auf bestimmte Container eingeschränkt werden, sodass sie sich nur auf die Objekte in diesen Containern auswirkt.


Assistent für neue Gruppenfamilie
Ort der verwalteten Objekte
Gruppe der verwalteten Objekte nach Ort definieren. Die Gruppenfamilie verwaltet nur die Objekte, die sich in den angegebenen Containern befinden.
Geben Sie Container zur Aufnahme der Objekte an, die von der Gruppenfamilie in Gruppen zusammengestellt werden sollen.
Container:
Name
In Ordner
ResDomain
ResDomain.msk.qsft
Hinzufügen...
Entfernen
Eigenschaften
< Zurück
Weiter >
Abbrechen
Hilfe

Auf dieser Seite werden die Container aufgelistet, die in den Bereich der Gruppenfamilie eingeschlossen werden sollen. Jeder Eintrag in der Liste identifiziert einen Container mit Namen und stellt den Pfad zu seinem übergeordneten Container bereit.

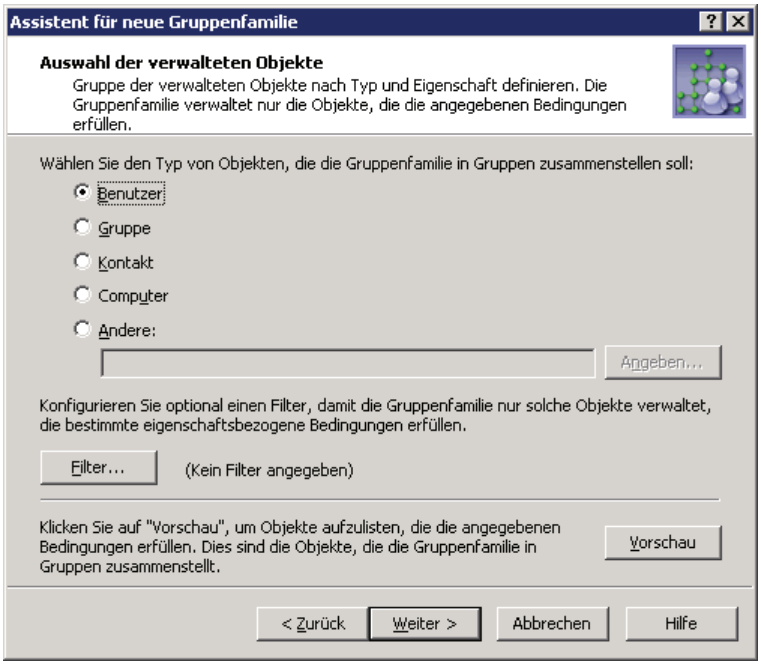
Um der Liste einen Container hinzuzufügen, klicken Sie auf **Hinzufügen** und wählen Sie den Container aus. Dann schließt der Gruppenfamilienbereich Objekte aus diesem Container ein.

Um Container aus der Liste zu entfernen, wählen Sie sie aus und klicken Sie dann auf **Entfernen**. Dann schließt der Gruppenfamilienbereich die Objekte aus diesen Containern nicht mehr ein.

Um Eigenschaften eines Containers anzuzeigen oder zu ändern, wählen Sie ihn in der Liste aus und klicken Sie auf **Eigenschaften**.

Auswahl der verwalteten Objekte

Auf der nächsten Seite werden Sie aufgefordert, den Typ der Objekte anzugeben, z.B. Benutzer oder Computer, die von der Gruppenfamilie verwaltet werden sollen. So wird der Bereich der Gruppenfamilie auf Objekte eines bestimmten Typs eingeschränkt. Um den Bereich weiter zu verfeinern, können Sie einen Filter anwenden, mit dem die Gruppenfamilie nur die Objekte verwaltet, die bestimmte Bedingungen in Bezug auf Eigenschaften erfüllen.


Assistent für neue Gruppenfamilie
Auswahl der verwalteten Objekte
Gruppe der verwalteten Objekte nach Typ und Eigenschaft definieren. Die Gruppenfamilie verwaltet nur die Objekte, die die angegebenen Bedingungen erfüllen.
Wählen Sie den Typ von Objekten, die die Gruppenfamilie in Gruppen zusammenstellen soll:
Benutzer
Gruppe
Kontakt
Computer
Andere:
Angeben...
Konfigurieren Sie optional einen Filter, damit die Gruppenfamilie nur solche Objekte verwaltet, die bestimmte eigenschaftsbezogene Bedingungen erfüllen.
Filter...
(Kein Filter angegeben)
Klicken Sie auf "Vorschau", um Objekte aufzulisten, die die angegebenen Bedingungen erfüllen. Dies sind die Objekte, die die Gruppenfamilie in Gruppen zusammenstellt.
Vorschau
< Zurück
Weiter >
Abbrechen
Hilfe

Sie können den Typ der Objekte auswählen, die in den Bereich der Gruppenfamilie eingeschlossen werden sollen:

- **Benutzer.** Der Bereich der Gruppenfamilie schließt nur Benutzerkonten ein.
- **Gruppe.** Der Bereich der Gruppenfamilie schließt nur Gruppen ein. Beachten Sie, dass die Gruppenfamilie bei dieser Option Gruppen erstellt und vorhandene Gruppen den neu erstellten Gruppen hinzufügt.
- **Kontakt.** Der Bereich der Gruppenfamilie schließt nur Kontaktobjekte ein.
- **Computer.** Der Bereich der Gruppenfamilie schließt nur Computerkonten ein.
- **Andere.** Der Bereich der Gruppenfamilie schließt nur Verzeichnisobjekte des ausgewählten Typs ein. Klicken Sie auf **Angeben** und wählen Sie einen Objekttyp aus.

Sie können den Gruppenfamilienbereich mit Hilfe eines Filters weiter verfeinern. Klicken Sie dazu auf **Filter**. Dann wird ein Fenster angezeigt, in dem Sie Filterkriterien anzeigen oder ändern können. Die Beschriftung neben der Schaltfläche **Filter** zeigt visuell an, ob Filterkriterien angegeben sind.

Im Fenster **Filter** können Sie eine Liste von Filterkriterien einrichten. Diese werden auch als *Bedingungen* bezeichnet. Jede Bedingung gibt eine Eigenschaft, einen Operator und einen Wert an. Je nach dem aktuellen Wert der Eigenschaft wird sie zu TRUE oder FALSE ausgewertet. Beispielsweise wird die folgende Bedingung für alle Objekte zu TRUE ausgewertet, bei denen die Beschreibung angibt, dass es sich um einen Vollzeitmitarbeiter handelt:

EIGENSCHAFT	BEDINGUNG	WERT
Beschreibung	Beginnt mit	Vollzeitkraft

Wenn Bedingungen angegeben sind, wird ein Filter angewendet, sodass der Bereich der Gruppenfamilie nur die Objekte einschließt, für die alle Bedingungen zu TRUE ausgewertet werden.

Wenn die Liste der Bedingungen leer ist, schließt der Bereich der Gruppenfamilie alle Objekte des angegebenen Typs ein, die in den angegebenen Containern enthalten sind. Es wird also keine Filterung angewendet.

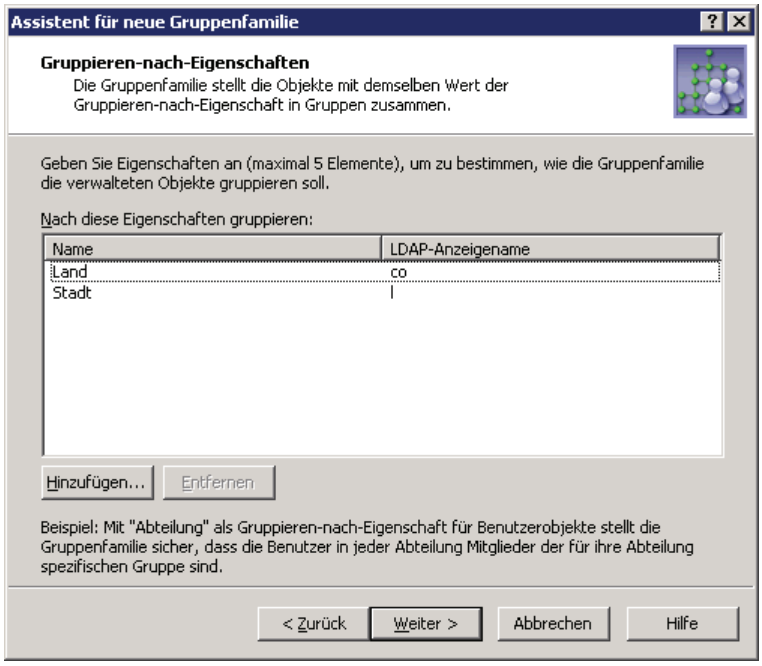
Wenn Sie einen Filter anwenden, werden nur die Objekte, die den Filterbedingungen entsprechen, zu den kontrollierten Gruppen hinzugefügt. Standardmäßig wird kein Filter angewandt, wodurch die kontrollierten Gruppen alle Objekte des angegebenen Typs enthalten. Sie können einen Standardfilter konfigurieren, indem Sie Eigenschaften auswählen und Bedingungen und Werte angeben, nach denen in den ausgewählten Eigenschaften gesucht werden soll.

Darüber hinaus haben Sie die Möglichkeit, einen erweiterten Filter zu konfigurieren, indem Sie eine entsprechende LDAP-Abfrage eingeben. Klicken Sie hierzu auf die Schaltfläche **Erweitert** im Fenster **Filter**. Beachten Sie, dass die Standard- und erweiterten Filteroptionen sich gegenseitig ausschließen. Wenn Sie einen erweiterten Filter angewandt haben, werden die Standardfiltereinstellungen ignoriert. Um zur Standardfilteroption zurückzukehren, klicken Sie auf die Schaltfläche **Standard** im Fenster „Filter". Hierdurch hat die Standardfilteroption wieder Vorrang vor der LDAP-Abfrage, auf der der erweiterte Filter basiert.

Sie können auf **Vorschau** auf der Seite **Auswahl der verwalteten Objekte** klicken, um eine Liste der Objekte anzuzeigen, die aktuell in den Gruppenfamilienbereich eingeschlossen sind. Im Fenster **Vorschau** werden die Objekte aufgelistet, die die Gruppenfamilie in Gruppen zusammenstellt.

Gruppieren-nach-Eigenschaften

Auf der nächsten Seite können Sie die Liste der Gruppieren-nach-Eigenschaften einrichten. Die Gruppenfamilie teilt die verwalteten Objekte (den Bereich) in Gruppierungen ein. Jede Gruppierung besteht aus den Objekten, bei denen die angegebenen Gruppieren-nach-Eigenschaften die gleiche Kombination von Werten aufweisen. Wenn beispielsweise die Abteilungseigenschaft als Gruppieren-nach-Eigenschaft für Benutzerobjekte angegeben ist, enthält jede Gruppierung nur die Benutzer aus einer bestimmten Abteilung. Dann stellt die Gruppenfamilie sicher, dass die Mitglieder jeder Gruppierung zu der Gruppe gehören, die mit der Gruppierung verknüpft ist.

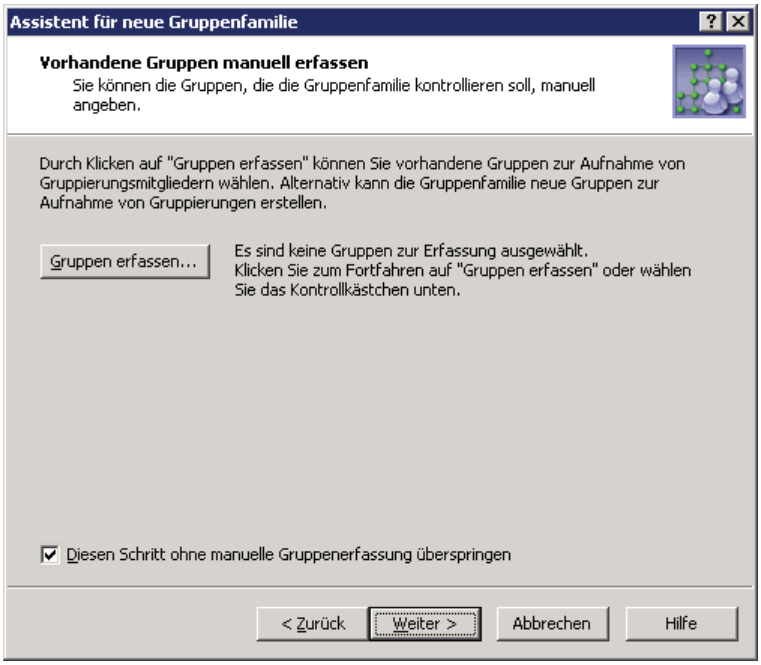

Assistent für neue Gruppenfamilie
Gruppieren-nach-Eigenschaften
Die Gruppenfamilie stellt die Objekte mit demselben Wert der Gruppieren-nach-Eigenschaft in Gruppen zusammen.
Geben Sie Eigenschaften an (maximal 5 Elemente), um zu bestimmen, wie die Gruppenfamilie die verwalteten Objekte gruppieren soll.
Nach diese Eigenschaften gruppieren:
Name
LDAP-Anzeigename
Land
co
Stadt
Hinzufügen...
Entfernen
Beispiel: Mit "Abteilung" als Gruppieren-nach-Eigenschaft für Benutzerobjekte stellt die Gruppenfamilie sicher, dass die Benutzer in jeder Abteilung Mitglieder der für ihre Abteilung spezifischen Gruppe sind.
< Zurück
Weiter >
Abbrechen
Hilfe

Auf der Seite werden die aktuell ausgewählten Gruppieren-nach-Eigenschaften aufgelistet. Sie können Eigenschaften der Liste hinzufügen oder aus ihr entfernen.

Die Änderungen, die Sie an der Liste auf dieser Seite vornehmen, legen die Gruppenfamilienoptionen neu fest, die von den Gruppieren-nach-Eigenschaften abhängig sind. Zu diesen Optionen gehören die Gruppenbenennungsregeln und die Liste der zu erfassenden Gruppen (wie in den folgenden beiden Abschnitten beschrieben). Wenn Sie eine Gruppieren-nach-Eigenschaft hinzufügen oder entfernen, werden die aktuellen Benennungsregeln durch die Standardbenennungsregel ersetzt, und die Liste der zu erfassenden Gruppen wird gelöscht.

Vorhandene Gruppen manuell erfassen

Auf der nächsten Seite können Sie vorhandene Gruppen mit Gruppierungen verknüpfen. Normalerweise erstellt die Gruppenfamilie automatisch eine Gruppe für jede Gruppierung und verknüpft sie mit ihr. Um dieses Verhalten für bestimmte Gruppierungen außer Kraft zu setzen, können Sie die Gruppenfamilie so konfigurieren, dass diese Gruppierungen mit den vorhandenen Gruppen verknüpft werden, die Sie angeben.


Assistent für neue Gruppenfamilie
Vorhandene Gruppen manuell erfassen
Sie können die Gruppen, die die Gruppenfamilie kontrollieren soll, manuell angeben.
Durch Klicken auf "Gruppen erfassen" können Sie vorhandene Gruppen zur Aufnahme von Gruppierungsmitgliedern wählen. Alternativ kann die Gruppenfamilie neue Gruppen zur Aufnahme von Gruppierungen erstellen.
Gruppen erfassen...
Es sind keine Gruppen zur Erfassung ausgewählt. Klicken Sie zum Fortfahren auf "Gruppen erfassen" oder wählen Sie das Kontrollkästchen unten.
Diesen Schritt ohne manuelle Gruppenerfassung überspringen
< Zurück
Weiter >
Abbrechen
Hilfe

Führen Sie auf dieser Seite eine der folgenden Aktionen aus:

- Damit die Gruppenfamilie automatisch für jede erkannte Gruppierung eine Gruppe erstellt und sie mit der Gruppierung verknüpft, aktivieren Sie das Kontrollkästchen **Diesen Schritt ohne manuelle Gruppenerfassung überspringen**.
- Um mindestens eine Verknüpfung zwischen Gruppe und Gruppierung manuell einzurichten, klicken Sie auf **Gruppen erfassen**.

Wenn Sie auf **Gruppen erfassen** klicken, wird ein Fenster angezeigt, in dem Sie eine Liste von Verknüpfungen zwischen Gruppe und Gruppierung anzeigen oder ändern können. Jeder Eintrag in der Liste schließt die folgenden Informationen ein:

- **Kombination von Werten der „Gruppieren-nach-Eigenschaften".** Die Kombination von Eigenschaftswerten, die eine Gruppierung identifiziert.
- **Gruppenname.** Identifiziert die Gruppe, die mit der Gruppierung verknüpft ist.
- **In Ordner.** Der kanonische Name des Containers, der die Gruppe enthält.

Das Fenster **Gruppen erfassen** umfasst die folgenden Schaltflächen für die Verwaltung der Liste von Verknüpfungen zwischen Gruppe und Gruppierung:

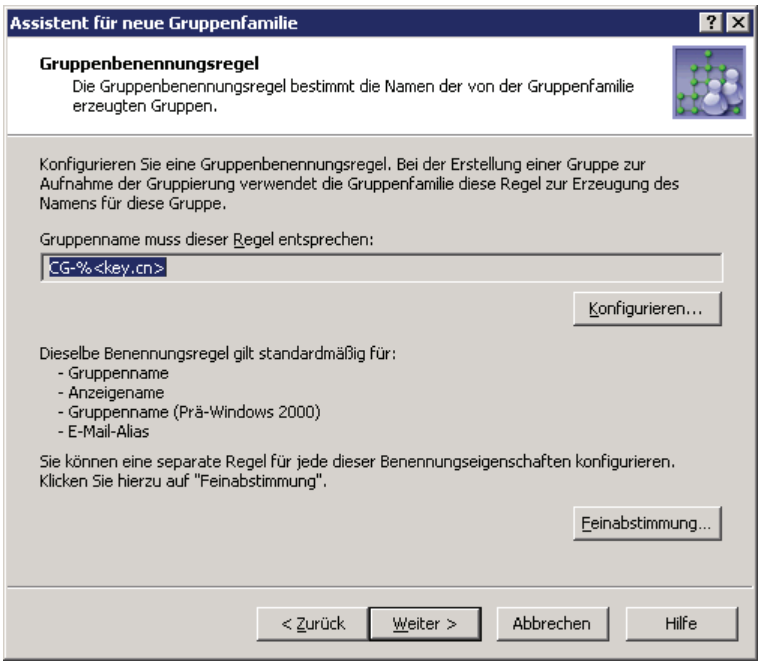
- **Hinzufügen.** Öffnet ein Fenster, in dem Sie eine Gruppe auswählen und eine Gruppierung angeben können. Um eine Gruppierung anzugeben, müssen Sie einen bestimmten Wert jeder der Gruppieren-nach-Eigenschaften eingeben. Dann wird die ausgewählte Gruppe mit der Gruppierung verknüpft, die durch die eingegebene Wertekombination identifiziert wird.

- **Bearbeiten.** Ermöglicht das Ändern eines Eintrags, den Sie in der Liste auswählen. Öffnet ein Fenster, in dem Sie eine andere Gruppe auswählen können oder eine andere Gruppierung angeben können, indem Sie die Wertekombination der Gruppieren-nach-Eigenschaften ändern.
- **Entfernen.** Löscht die ausgewählten Verknüpfungen aus der Liste. Die Gruppenfamilie erstellt dann neue Gruppen für die Gruppierungen, die Sie aus der Liste entfernt haben.

Gruppenbenennungsregel

Auf der nächsten Seite des Assistenten können Sie die von der Gruppenfamilie verwendeten Gruppenbenennungsregeln anzeigen oder ändern.

Beim Erstellen einer neuen Gruppe generiert die Gruppenfamilie die Gruppenbenennungseigenschaften, z.B. den Gruppennamen, den Anzeigenamen, den Gruppennamen (Prä-Windows 2000) und optional den E-Mail-Alias. Falls nichts anderes angegeben ist, verwendet die Gruppenfamilie eine bestimmte Standardregel, um diese Eigenschaften anhand der Werte der Gruppieren-nach-Eigenschaften zu generieren.


Assistent für neue Gruppenfamilie
Gruppenbenennungsregel
Die Gruppenbenennungsregel bestimmt die Namen der von der Gruppenfamilie erzeugten Gruppen.
Konfigurieren Sie eine Gruppenbenennungsregel. Bei der Erstellung einer Gruppe zur Aufnahme der Gruppierung verwendet die Gruppenfamilie diese Regel zur Erzeugung des Namens für diese Gruppe.
Gruppenname muss dieser Regel entsprechen:
CG-%<key.cn>
Konfigurieren...
Dieselbe Benennungsregel gilt standardmäßig für:
- Gruppenname
- Anzeigename
- Gruppenname (Prä-Windows 2000)
- E-Mail-Alias
Sie können eine separate Regel für jede dieser Benennungseigenschaften konfigurieren. Klicken Sie hierzu auf "Feinabstimmung".
Feinabstimmung...
< Zurück
Weiter >
Abbrechen
Hilfe

Standardmäßig generiert die Gruppenfamilie die Gruppenbenennungseigenschaften anhand der folgenden Syntax: CG-%<Schlüssel.Eigenschaft1>-%<Schlüssel.Eigenschaft2>... In dieser Syntax steht CG für „Gruppieren nach Eigenschaft" dar, und die %<...>-Einträge repräsentieren den Wert einer Eigenschaft der bestimmten Gruppierung. Beim Erstellen einer Gruppe für eine bestimmte Gruppierung setzt die Gruppenfamilie den gruppierungsspezifischen Wert der „Gruppieren-nach" Eigenschaft in den Eintrag mit dem Namen dieser Eigenschaft ein. Beispielsweise wird in einer Gruppe, die durch den Wert **Operations (Betrieb)** der Eigenschaft **Department** identifiziert wird, der Gruppenname auf **CG-Vorgänge festgelegt**. Bei zwei Gruppieren-nach-Eigenschaften wie etwa **Department** und **Stadt** lautet ein Beispiel für den Gruppennamen **CG-Operations-London**.

Um die Gruppenbenennungsregel zu ändern, klicken Sie auf die Schaltfläche **Konfigurieren**. Hierdurch wird das Dialogfeld **Wert konfigurieren** geöffnet, das weiter oben in diesem Dokument beschrieben wurde (siehe „Konfigurieren einer Richtlinie für die Generierung und Validierung von Eigenschaften"). In diesem Dialogfeld können Sie einen Wert für die Bedingung **'Name' muss sein** konfigurieren, ähnlich wie beim Konfigurieren der Richtlinie „Erzeugung und Validierung von Eigenschaften".

Ein Wert entsteht durch Verkettung von mindestens einem Eintrag. Im Dialogfeld **Wert konfigurieren** befinden sich die Schaltflächen **Hinzufügen**, **Bearbeiten** und **Entfernen** für die Verwaltung der Eintragsliste. Durch Klicken auf **Hinzufügen** wird das Fenster **Eintrag hinzufügen** angezeigt.

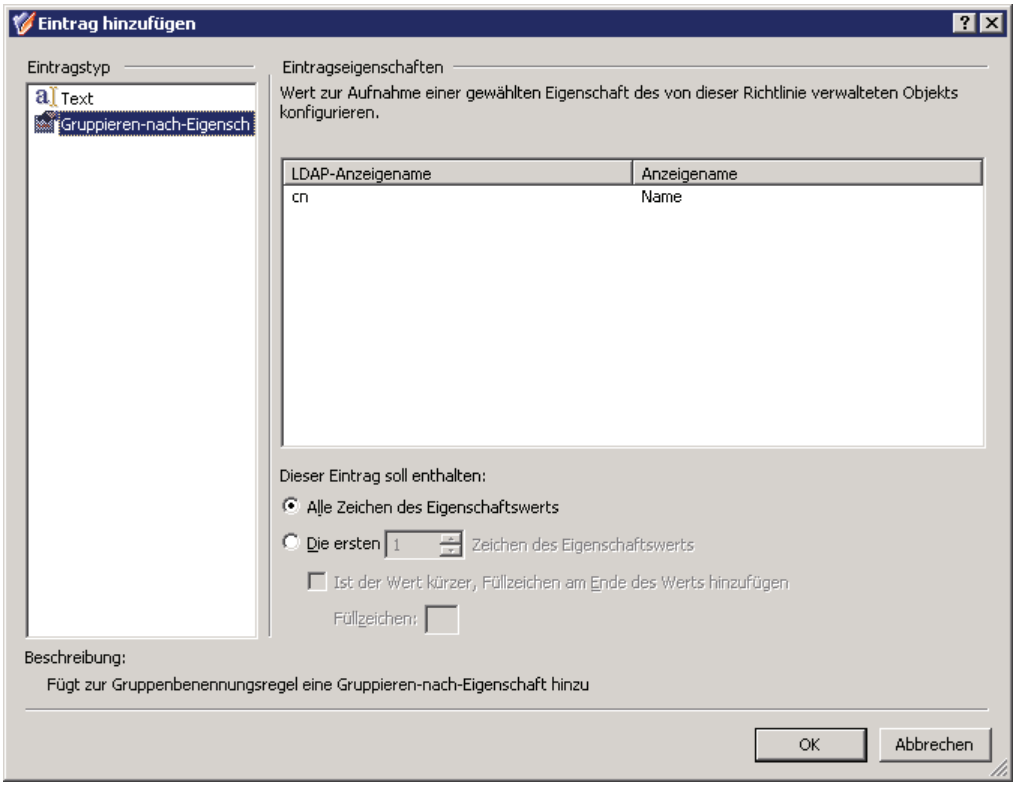
Im Fenster **Eintrag hinzufügen** können Sie den Typ des hinzuzufügenden Eintrags auswählen und den Eintrag dann konfigurieren. Folgende Eintragstypen sind verfügbar:

- **Text.** Fügt der Gruppenbenennungsregel eine Textzeichenfolge hinzu.
- **Gruppieren-nach-Eigenschaft.** Fügt der Gruppenbenennungsregel eine Gruppieren-nach-Eigenschaft oder einen Teil einer Gruppieren-nach-Eigenschaft hinzu.

Um eine Textzeichenfolge hinzuzufügen, geben Sie einfach im Fenster **Eintrag hinzufügen** einen Text ein. Im folgenden Unterabschnitt wird der Eintrag **Gruppieren-nach-Eigenschaft** erörtert.

Eintragstyp: Gruppieren-nach-Eigenschaft

Wenn Sie im Fenster **Eintrag hinzufügen** unter **Eintragstyp** den Typ **Gruppieren-nach-Eigenschaft** auswählen, ähnelt der Bereich **Eintragseigenschaften** der folgenden Abbildung.



Mit Hilfe des Eintragstyps **Gruppieren-nach-Eigenschaft** können Sie einen Eintrag hinzufügen, der einen Wert (oder einen Teil eines Werts) einer „Gruppieren-nach" Eigenschaft darstellt. Wählen Sie in der Liste eine Gruppieren-nach-Eigenschaft aus, und führen Sie dann eine der folgenden Aktionen aus:

- Wenn der Eintrag den gesamten Wert der Eigenschaft enthalten soll, klicken Sie auf **Alle Zeichen des Eigenschaftswerts**.
- Wenn der Eintrag einen Teil des Eigenschaftswerts enthalten soll, klicken Sie auf **Die ersten** und geben Sie an, wie viele Zeichen in den Eintrag eingeschlossen werden sollen.

Wenn Sie die zweite Option auswählen, können Sie das Kontrollkästchen **Ist der Wert kürzer, Füllzeichen am Ende des Werts hinzufügen** aktivieren und ein Zeichen in das Feld **Füllzeichen** eingeben. Dieses Zeichen ersetzt die fehlenden Zeichen im Wert der Eigenschaft, wenn dieser Wert kürzer ist als im Feld neben der Option **Die ersten** angegeben. Wenn Sie beispielsweise **Die ersten 12 Zeichen** angeben und **0** als Füllzeichen eingeben, wird aus dem Eigenschaftswert **Accounting** der Eintrag **Accounting00**.

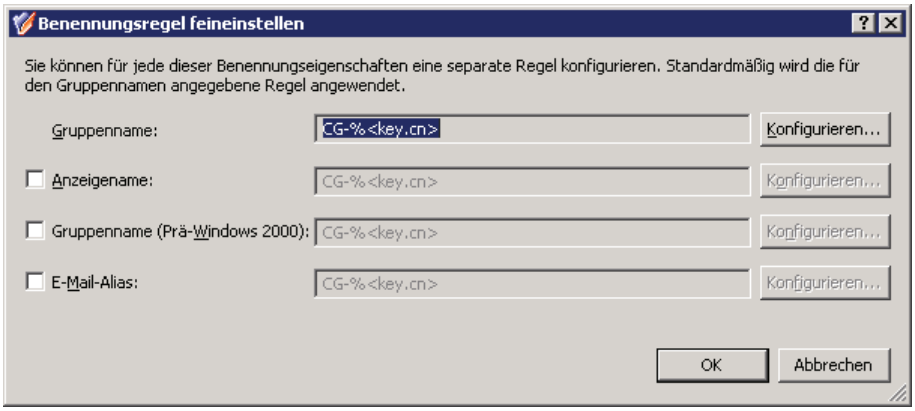
Klicken Sie nach dem Konfigurieren eines Eintrags auf **OK**, um das Fenster **Eintrag hinzufügen** zu schließen. Der Eintrag wird dem Dialogfeld **Wert konfigurieren** hinzugefügt. Klicken Sie nach dem Abschließen der Eintragsliste auf **OK**, um das Dialogfeld zu schließen. Beachten Sie, dass die Benennungsregel für jede Gruppieren-nach-Eigenschaft einen Eintrag enthalten muss.

Unterschiedliche Regeln für die Benennungseigenschaften

Standardmäßig gilt dieselbe Regel für die folgenden Benennungseigenschaften:

- Gruppenname
- Gruppenname (Prä-Windows 2000)
- Gruppenanzeigename
- E-Mail-Alias (wenn die Gruppenfamilie für die Erstellung E-Mail-fähiger Gruppen konfiguriert ist, wie weiter unten in diesem Kapitel beschrieben)

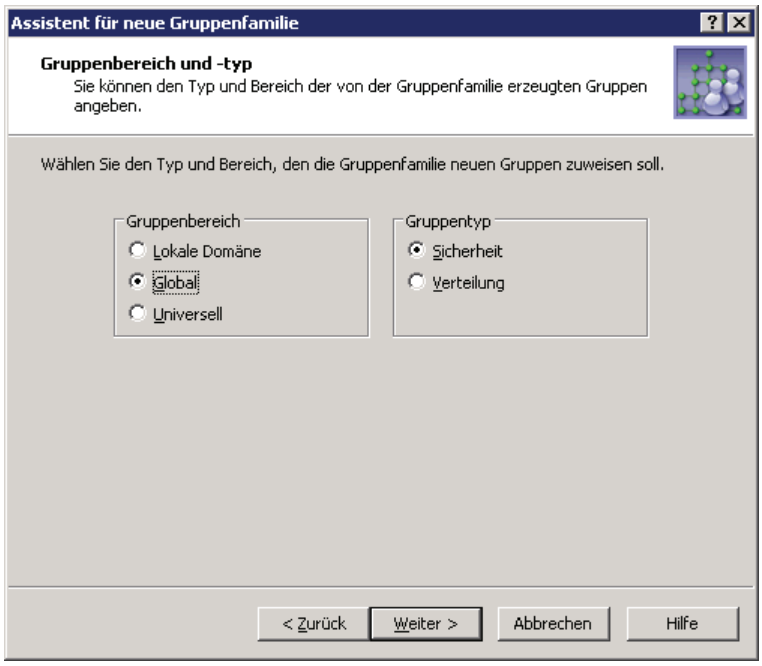
Sie können für jede dieser Benennungseigenschaften eine eigene Regel konfigurieren. Klicken Sie dazu auf der Seite **Gruppenbenennungsregel** auf **Feinabstimmung**. Dann wird ein Fenster angezeigt, in dem Sie eine Benennungseigenschaft auswählen und eine Regel für diese Eigenschaft (wie für einen Gruppennamen) konfigurieren können. Das Fenster ähnelt der folgenden Abbildung.



Möglicherweise müssen Sie für eine bestimmte Eigenschaft eine separate Regel konfigurieren und dabei Einschränkungen beachten, die für diese Eigenschaft gelten. Beispielsweise muss der Gruppenname (Prä-Windows 2000) weniger als 20 Zeichen lang sein. Um diese Anforderung zu erfüllen, aktivieren Sie das Kontrollkästchen **Gruppenname (Prä-Windows 2000)** und klicken Sie auf **Konfigurieren**, um eine entsprechende Regel einzurichten. Wenn Sie Einträge so konfigurieren, dass sie Gruppieren-nach-Eigenschaften einschließen, begrenzen Sie die Anzahl der Zeichen in jedem Eintrag mit Hilfe der Option **Die ersten** im Fenster **Eintrag hinzufügen**.

Gruppenbereich und -typ

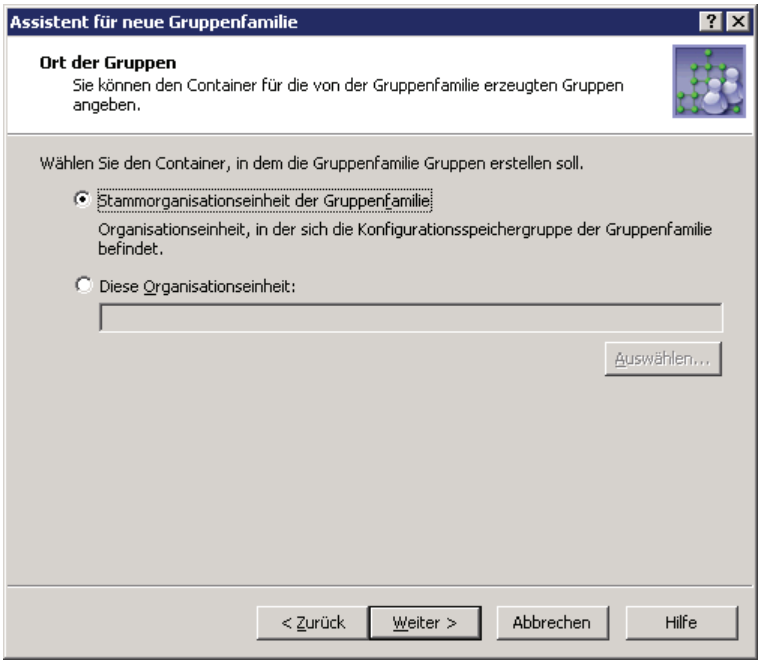
Auf der nächsten Seite können Sie den Gruppenbereich und typ angeben, der den von der Gruppenfamilie generierten Gruppen zugewiesen werden soll.



Verfügbar sind die Standardoptionen für den Gruppenbereich und den Gruppentyp. Die Gruppenfamilie erstellt Gruppen mit dem Bereich und Typ, den Sie auswählen.

Ort der Gruppen

Auf der nächsten Seite können Sie den Container angeben, der die von der Gruppenfamilie generierten Gruppen enthalten soll.

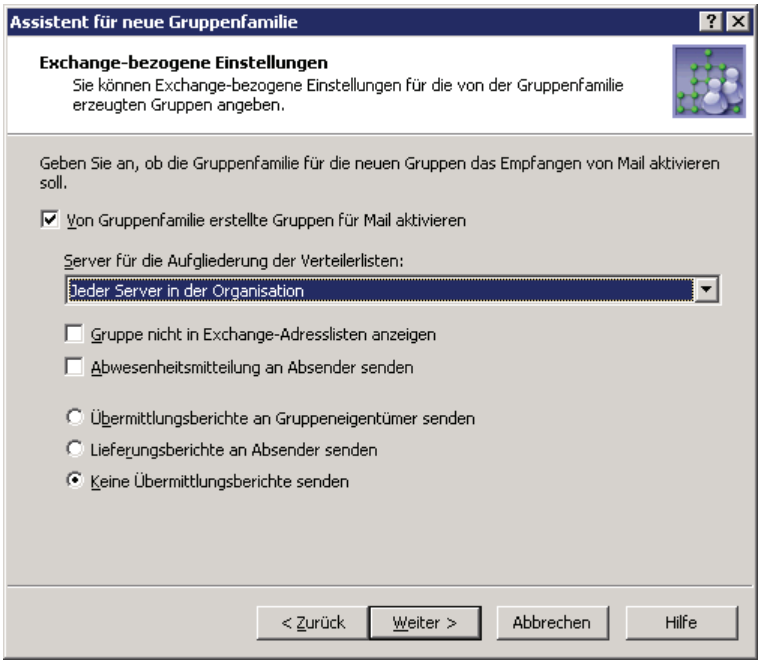

Assistent für neue Gruppenfamilie
Ort der Gruppen
Sie können den Container für die von der Gruppenfamilie erzeugten Gruppen angeben.
Wählen Sie den Container, in dem die Gruppenfamilie Gruppen erstellen soll.
Stammorganisationseinheit der Gruppenfamilie
Organisationseinheit, in der sich die Konfigurationsspeichergruppe der Gruppenfamilie befindet.
Diese Organisationseinheit:
Auswählen...
< Zurück
Weiter >
Abbrechen
Hilfe

Sie können eine der folgenden Optionen auswählen:

- **Stammorganisationseinheit der Gruppenfamilie.** Die Gruppenfamilie erstellt Gruppen in dem Container, in dem sich die Konfigurationsspeichergruppe für diese Gruppenfamilie befindet (siehe „Starten des Assistent für neue Gruppenfamilie" weiter oben in diesem Kapitel).
- **Diese Organisationseinheit.** Die Gruppenfamilie erstellt Gruppen in dem angegebenen Container. Klicken Sie zur Auswahl eines Containers auf **Auswählen**.

Exchange-bezogene Einstellungen

Auf der nächsten Seite können Sie angeben, ob die von der Gruppenfamilie generierten Gruppen E-Mail-fähig sein sollen. Außerdem können Sie Eigenschaften im Zusammenhang mit Exchange einrichten, die diesen Gruppen bei ihrer Erstellung zugewiesen werden sollen.


Assistent für neue Gruppenfamilie
Exchange-bezogene Einstellungen
Sie können Exchange-bezogene Einstellungen für die von der Gruppenfamilie erzeugten Gruppen angeben.
Geben Sie an, ob die Gruppenfamilie für die neuen Gruppen das Empfangen von Mail aktivieren soll.
Von Gruppenfamilie erstellte Gruppen für Mail aktivieren
Server für die Aufgliederung der Verteilerlisten:
Jeder Server in der Organisation
Gruppe nicht in Exchange-Adresslisten anzeigen
Abwesenheitsmitteilung an Absender senden
Übermittlungsberichte an Gruppeneigentümer senden
Lieferungsberichte an Absender senden
Keine Übermittlungsberichte senden
< Zurück
Weiter >
Abbrechen
Hilfe

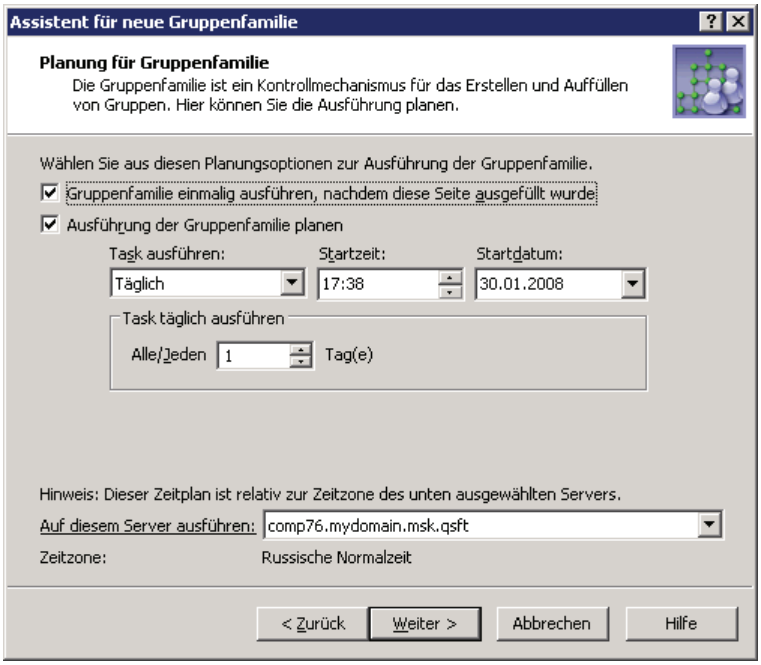
Wenn die Gruppen der Gruppenfamilie E-Mail-fähig sein sollen, aktivieren Sie das Kontrollkästchen **Von Gruppenfamilie erstellte Gruppen für Mail aktivieren**. Dann können Sie die folgenden Eigenschaften im Zusammenhang mit Exchange für die Gruppen der Gruppenfamilie einrichten:

- **Server für die Aufgliederung der Verteilerlisten.** Der Exchange-Server, mit dem eine Gruppe der Gruppenfamilie zu einer Liste von Gruppenmitgliedern erweitert wird.
- **Gruppe nicht in Exchange-Adresslisten anzeigen.** Verhindert, dass die Gruppen der Gruppenfamilie in Adressenlisten angezeigt werden. Wenn Sie dieses Kontrollkästchen aktivieren, werden alle Gruppen in allen Adressenlisten ausgeblendet.
- **Abwesenheitsmitteilung an Absender senden.** Aktivieren Sie dieses Kontrollkästchen, wenn Sie möchten, dass Abwesenheitsbenachrichtigungen an den Urheber der Nachricht gesendet werden, wenn eine Nachricht an eine Gruppe in der Gruppenfamilie gesendet wird und mindestens ein Gruppenmitglied eine Abwesenheitsbenachrichtigung aktiviert hat.
- **Übermittlungsberichte an Gruppeneigentümer senden.** Verwenden Sie diese Option, wenn Sie möchten, dass Übermittlungsberichte an den Gruppenbesitzer gesendet werden, wenn eine Nachricht an eine Gruppe in der Gruppenfamilie nicht übermittelt werden kann. So wird der Gruppenbesitzer darüber informiert, dass die Nachricht nicht übermittelt wurde.
- **Lieferungsberichte an Absender senden.** Verwenden Sie diese Option, wenn Sie möchten, dass Übermittlungsberichte an den Urheber der Nachricht gesendet werden, wenn eine Nachricht an eine Gruppe in der Gruppenfamilie nicht übermittelt werden kann. So wird der Urheber der Nachricht darüber informiert, dass die Nachricht nicht übermittelt wurde.
- **Keine Übermittlungsberichte senden.** Verwenden Sie diese Option, wenn Sie nicht möchten, dass Übermittlungsberichte gesendet werden, selbst wenn eine Nachricht an eine Gruppenfamilie nicht übermittelt werden kann.

Planung für Gruppenfamilie

Auf der nächsten Seite können Sie die Ausführungen der Gruppenfamilie planen. Während jeder Ausführung verhält sich die Gruppenfamilie wie im Abschnitt „Funktionsweise" weiter oben in diesem Kapitel beschrieben.

Beachten Sie beim Einrichten der Zeitplanoptionen, dass eine Ausführung der Gruppenfamilie lange dauert und viele Ressourcen beansprucht. Daher sollte sie für einen Zeitraum geplant werden, in dem sie möglichst geringe Auswirkungen auf Benutzer hat.



Aktivieren Sie das erste Kontrollkästchen, um die Gruppenfamilie direkt nach Abschluss des Assistenten und immer dann, wenn die Gruppenfamilie durch die Verwaltung der Konfigurationsspeichergruppe geändert wird, auszuführen (siehe „Verwalten einer Gruppenfamilie" weiter unten in diesem Kapitel).

Aktivieren Sie das zweite Kontrollkästchen, um Zeitplanoptionen einzurichten. Wenn dieses Kontrollkästchen aktiviert ist, wird die Gruppenfamilie zu angegebenen Zeiten ausgeführt.

In der Liste **Auf diesem Server ausführen** können Sie den Verwaltungsdienst auswählen, mit dem die Gruppenfamilie ausgeführt werden soll. Sie sollten den Dienst mit der geringsten Auslastung auswählen.

Zusammenfassung: Verfahren zur Erstellung einer Gruppenfamilie

Die Erstellung einer Gruppenfamilie besteht aus den folgenden zwei Schritten:

1. Erstellen der Gruppenfamilienkonfiguration
2. Ausführen der Gruppenfamilie zur Erstellung oder Erfassung von Gruppen

Die Quest One ActiveRoles-Konsole enthält den Assistenten „Neue Gruppenfamilie", mit dem Sie die Gruppenfamilienkonfiguration erstellen können. Der Assistent erstellt eine Gruppe, die als *Konfigurationsspeichergruppe* bezeichnet wird, und füllt sie mit den von Ihnen angegebenen Konfigurationsdaten auf. Der Assistent ermöglicht Ihnen auch, die Gruppenfamilie sofort auszuführen oder die Ausführung der Gruppenfamilie auf regelmäßiger Basis zu planen.

Gehen Sie folgendermaßen vor, um die Gruppenfamilienkonfiguration zu erstellen und die Gruppenfamilie auszuführen:

1. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf die Organisationseinheit, in der Sie Gruppenfamilien-Konfigurationsspeichergruppe erstellen möchten, und wählen Sie **Neu | Gruppenfamilie** aus, um den Assistenten zur Erstellung einer neuen Gruppenfamilie zu starten.
2. Folgen Sie den Anweisungen des Assistenten.
3. Geben Sie auf der Seite **Gruppenfamilie benennen** einen Namen für die Gruppenfamilie ein.

   Der Assistent erstellt die Gruppenfamilien-Konfigurationsspeichergruppe mit dem Namen, den Sie auf dieser Seite angegeben haben.
4. Führen Sie auf der Seite **Gruppierungsoptionen** einen der folgenden Vorgänge aus und klicken Sie dann auf **Weiter**.
   - Klicken Sie auf **Vorkonfigurierte Gruppierung nach** und wählen Sie dann vorkonfigurierte Gruppierungskriterien aus der Liste aus.
   - Klicken Sie auf **Benutzerdefinierte Gruppierung**, um benutzerdefinierte Gruppierungskriterien in den folgenden Assistentenschritten zu konfigurieren.
5. Führen Sie auf der Seite **Ort der verwalteten Objekte** einen der folgenden Vorgänge aus und klicken Sie dann auf **Weiter**:
   - Klicken Sie auf **Hinzufügen** und wählen Sie dann einen Container, der die in Gruppen zusammenzuführenden Objekte enthält.
   - Klicken Sie auf **Entfernen**, um einen ausgewählten Container aus der Liste **Container** zu entfernen.
6. Führen Sie auf der Seite **Auswahl der verwalteten Objekte** einen der folgenden Vorgänge aus und klicken Sie dann auf **Weiter**:
   - Wählen Sie einen Objekttyp durch Anklicken von einer der vier obersten Optionen aus; oder klicken Sie auf **Sonstige** und dann auf **Festlegen**, um einen Objekttyp aus der Liste **Objekttypen** auszuwählen.
   - Klicken Sie auf **Filter** und füllen das Dialogfeld **Filter** anhand der weiter unten in diesem Thema aufgeführten Verfahrensweise aus.
   - Klicken Sie auf **Vorschau**, um die Liste von Objekten anzuzeigen, die den festgelegten Bedingungen entsprechen.
7. Gehen Sie auf der Seite **Gruppieren-nach Eigenschaft** wie nachfolgend beschrieben vor und klicken Sie dann auf **Weiter**:
   - Klicken Sie auf **Hinzufügen** und wählen Sie eine Objekteigenschaft aus der Liste **Objekteigenschaft** aus.

8. Wählen Sie auf der Seite **Vorhandene Gruppen manuell erfassen** die Option **Diesen Schritt ohne manuelle Gruppenerfassung überspringen** aus und klicken Sie dann auf **Weiter**.
9. Gehen Sie auf der Seite **Gruppenbenennungsregel** wie nachfolgend beschrieben vor und klicken Sie dann auf **Weiter**.
    - Klicken Sie auf **Konfigurieren** und füllen das Dialogfeld **Wert konfigurieren** anhand der weiter unten in diesem Thema aufgeführten Verfahrensweise aus.
    - Klicken Sie auf **Benennungsregel fein einstellen** und füllen das Dialogfeld **Benennungsregel fein einstellen** anhand der weiter unten in diesem Thema aufgeführten Verfahrensweise aus.
10. Gehen Sie auf der Seite **Gruppentyp und umfang** wie nachfolgend beschrieben vor und klicken Sie dann auf **Weiter**:
    - Wählen Sie im Bereich **Gruppenausmaß** ein Gruppenausmaß aus.
    - Wählen Sie im Bereich **Gruppentyp** einen Gruppentyp aus.
11. Führen Sie auf der Seite **Ort der Gruppen** einen der folgenden Vorgänge aus und klicken Sie dann auf **Weiter**:
    - Damit die Gruppenfamilie neue Gruppen in der Organisationseinheit erstellt, in der sich die Gruppenfamilien-Konfigurationsspeichergruppe befindet, klicken Sie auf **Stammorganisationseinheit der Gruppenfamilie**.
    - Damit die Gruppenfamilie neue Gruppen in einer anderen Organisationseinheit erstellt, klicken Sie auf **Diese Organisationseinheit** und klicken Sie dann auf **Wählen**, um die Organisationseinheit auszuwählen.
12. Gehen Sie auf der Seite **Exchange-bezogene Einstellungen** wie nachfolgend beschrieben vor und klicken Sie dann auf **Weiter**:
    - Aktivieren oder deaktivieren Sie das Kontrollkästchen **Von der Gruppenfamilie erstellte Gruppen E-Mail-aktivieren**. Wenn Sie dieses Kontrollkästchen aktivieren, konfigurieren Sie die Exchange-bezogenen Optionen auf dieser Seite.
13. Gehen Sie auf der Seite **Planung für Gruppenfamilie** wie nachfolgend beschrieben vor und klicken Sie dann auf **Weiter**:
    - Wenn die Gruppenfamilie nach Abschluss des Assistenten einmalig ausgeführt werden soll, wählen Sie **Gruppenfamilie einmalig ausführen, nachdem diese Seite ausgefüllt wurde**.
    - Wenn die Gruppenfamilie auf geplanter Basis ausgeführt werden soll, wählen Sie **Ausführung der Gruppenfamilie planen** und konfigurieren Sie dann das Datum, die Uhrzeit und das Intervall der Ausführungen mit Hilfe der Optionen unter diesem Kontrollkästchen.
    - Wählen Sie in der Liste **Auf diesem Server ausführen** den Verwaltungsdienst aus, der die Gruppenfamilie ausführen soll.
14. Klicken Sie auf der letzten Seite des Assistenten auf **Fertig stellen**.

Gehen Sie folgendermaßen vor, um das Dialogfeld „Filter" abzuschließen:

1. Wählen Sie unter **Eigenschaft wählen** eine Objekteigenschaft aus.
2. Wählen Sie im Dropdown-Listenfeld **Operator wählen** einen Operator aus.
3. In **Wert angeben (Groß-/Kleinschreibung muss nicht berücksichtigt werden)** geben Sie einen Wert für die ausgewählte Eigenschaft ein.
4. Klicken Sie auf **Hinzufügen**, um die Filterbedingung, die Sie gerade angegeben haben, zur Liste **Bedingungen** hinzuzufügen.
5. Um mehrere Filterbedingungen hinzuzufügen, wiederholen Sie die Schritte 1-4.

Gehen Sie folgendermaßen vor, um das Dialogfeld „Wert konfigurieren" abzuschließen:

1. Klicken Sie auf **Hinzufügen**.
2. Führen Sie im Dialogfeld **Eintrag hinzufügen** einen der folgenden Vorgänge durch und klicken Sie auf **OK**:
   - Um einen Texteintrag zu konfigurieren, klicken Sie auf **Text** unter **Eintragstyp** und geben Sie dann einen Wert in das Feld **Textwert** ein.
   - Um einen „Gruppieren-nach Eigenschaft"-Eintrag zu konfigurieren, klicken Sie auf **Gruppieren-nach-Eigenschaft** unter **Eintragstyp**, wählen Sie dann unter **Eintragseigenschaften** eine Eigenschaft aus der Liste aus und führen Sie einen der folgenden Vorgänge aus:
     - Wenn der Eintrag den gesamten Wert der Eigenschaft enthalten soll, klicken Sie auf **Alle Zeichen des Eigenschaftswerts**.
     - Wenn der Eintrag einen Teil des Eigenschaftswerts enthalten soll, klicken Sie auf **Die ersten** und geben Sie an, wie viele Zeichen in den Eintrag eingeschlossen werden sollen.
3. Sie können optional Folgendes vornehmen:
   - Fügen Sie weitere Einträge hinzu, löschen oder bearbeiten Sie vorhandene Einträge und verwenden Sie die Pfeilschaltflächen, um Einträge nach oben oder unten in der Liste zu verschieben.
   - Fügen Sie die Inhalte der Zwischenablage in die Eintragsliste ein, indem Sie auf die Schaltfläche neben dem Feld **Konfigurierter Wert** klicken.
4. Klicken Sie auf **OK**.

Gehen Sie folgendermaßen vor, um das Dialogfeld „Feinabstimmungsbenennungsregel" abzuschließen:

1. Aktivieren Sie das Kontrollkästchen und klicken Sie dann auf die Schaltfläche **Konfigurieren** neben der Namenseigenschaft, die Sie konfigurieren möchten, und vervollständigen Sie dann das Dialogfeld **Wert konfigurieren**, indem Sie das oben beschriebene Verfahren befolgen.
2. Klicken Sie auf **OK**.

Verwalten einer Gruppenfamilie

Die meisten Aufgaben im Zusammenhang mit der Gruppenfamilienverwaltung werden mit dem Befehl **Eigenschaften** für die Gruppen ausgeführt, in denen die Gruppenfamilienkonfigurationen gespeichert sind. Auf der Quest One ActiveRoles-Konsole sind solche Gruppen mit einem besonderen Symbol markiert, das sie von gewöhnlichen Gruppen unterscheidet.

Wenn Sie eine Gruppenfamilie erstellen, wird eine Gruppe erstellt, in der die Gruppenfamilienkonfiguration gespeichert wird. Der Gruppe wird der Name zugewiesen, den Sie für die Gruppenfamilie bereitgestellt haben, und sie wird mit dem Gruppenfamilien-Symbol markiert:

Um die Gruppenfamilienverwaltung zu erleichtern, enthält das Dialogfeld **Eigenschaften** für eine Konfigurationsspeichergruppe eine Reihe von Registerkarten speziell für Gruppenfamilien:

- **Registerkarte „Allgemein"**. Zeigt den Namen der Gruppenfamilie an, und ermöglicht dem Administrator, die Beschreibung, den Gruppentyp und den Gruppenbereich der Speichergruppe anzuzeigen oder zu ändern.
- **Registerkarte „Kontrollierte Gruppen"**. Listet die Gruppen auf, die von der Gruppenfamilie kontrolliert werden, und ermöglicht dem Administrator das Anzeigen und Ändern der Verknüpfungen zwischen Gruppe und Gruppierung sowie der Regeln im Zusammenhang mit der Gruppenerstellung.
- **Registerkarte „Gruppierungen"**. Ermöglicht dem Administrator das Anzeigen oder Ändern des Gruppenfamilienbereichs und der Liste von Gruppieren-nach-Eigenschaften.
- **Registerkarte „Zeitplan"**. Zeigt Informationen zum Zeitplan der Gruppenfamilie an und ermöglicht dem Administrator das Anzeigen oder Ändern von Zeitplanungseinstellungen.
- **Registerkarte „Vorgangsübersicht"**. Zeigt Informationen zur letzten Ausführung der Gruppenfamilie an und ermöglicht dem Administrator das Anzeigen eines detaillierten Protokolls zu den Ausführungsergebnissen.

Diese Registerkarten werden weiter unten in diesem Abschnitt detaillierter erörtert.

Änderungen an den gewöhnlichen, auf Gruppen bezogenen Eigenschaften der Konfigurationsspeichergruppe haben keine Auswirkungen auf die Gruppenfamilie. Beispielsweise können Sie die Konfigurationsspeichergruppe umbenennen oder verschieben, ohne dass Auswirkungen auf den Prozess und die Ergebnisse eines Gruppenfamilienvorgangs entstehen. Wenn Sie die Konfigurationsspeichergruppe umbenennen, wird nur der Anzeigename der Gruppenfamilie geändert.

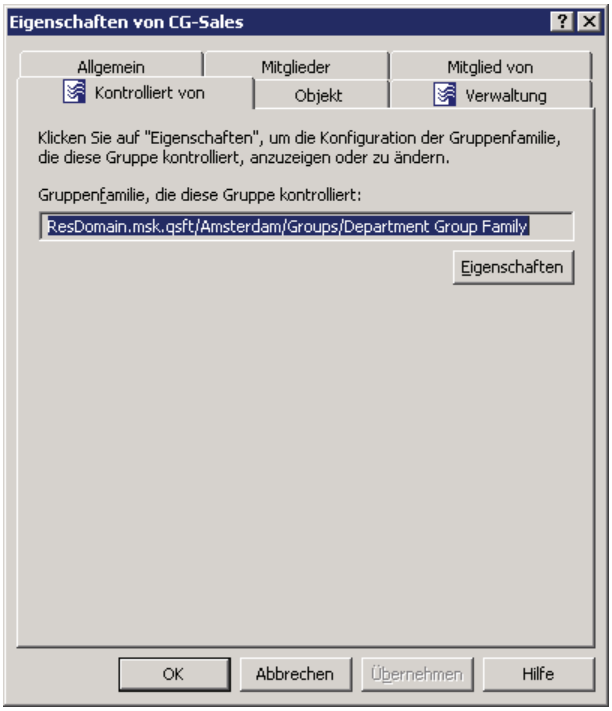
Das Menü **Aktion** in jeder Gruppenfamilien-Konfigurationsspeichergruppe enthält den Befehl **Ausführung erzwingen**, sodass Sie die Gruppenfamilie ausführen können, wenn Sie sie direkt aktualisieren möchten, ohne auf die geplante Ausführungszeit zu warten.

Kontrollierte Gruppen

Damit die Gruppen, die von einer Gruppenfamilie kontrolliert werden (die kontrollierten Gruppen) leichter zu erkennen sind, sind sie auf der Quest One ActiveRoles-Konsole mit einem besonderen Symbol markiert. So wird zum Beispiel das folgende Symbol verwendet, um eine globale Gruppe anzugeben, die unter der Kontrolle einer Gruppenfamilie steht:

Zusätzlich wird dem Feld **Hinweise** für solche Gruppen ein erklärender Text hinzugefügt, der angibt, dass die Gruppenfamilie alle Änderungen außer Kraft setzt, die direkt an der Gruppenmitgliedschaftsliste vorgenommen werden.

Auf der Quest One ActiveRoles-Konsole schließt das Dialogfeld **Eigenschaften** für kontrollierte Gruppen eine Registerkarte speziell für die Gruppenfamilie ein, die Registerkarte **Kontrolliert von**. Über diese Registerkarte können Sie die Konfiguration der Gruppenfamilie verwalten, die die Gruppe steuert:



Auf der Registerkarte **Kontrolliert von** werden der Pfad und der Name der Gruppenfamilien-Konfigurationsspeichergruppe angezeigt. Diese Registerkarte stellt einen Einstiegspunkt für die Gruppenfamilienverwaltung dar.

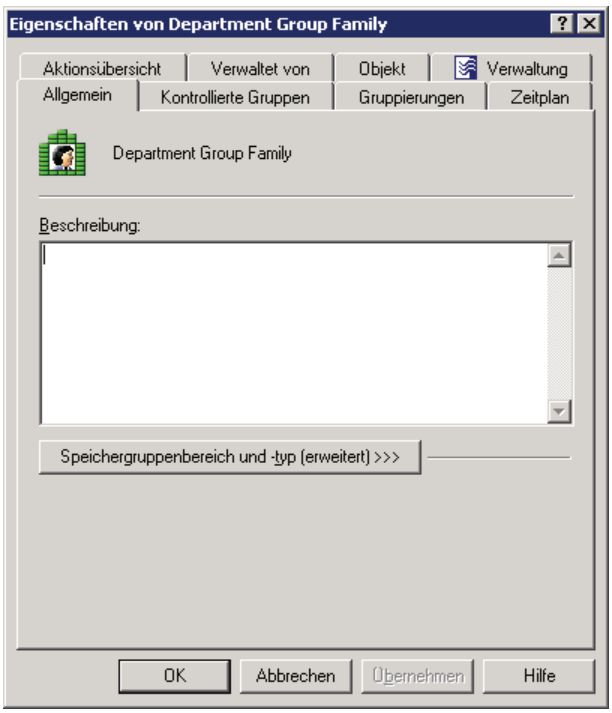
Es gibt also zwei Möglichkeiten, auf das Dialogfeld **Eigenschaften** der Gruppenfamilien-Konfigurationsspeichergruppe auf der Quest One ActiveRoles-Konsole zuzugreifen:

- Klicken Sie im Dialogfeld **Eigenschaften** für eine beliebige von der Gruppenfamilie kontrollierte Gruppe auf der Registerkarte **Kontrolliert von** auf **Eigenschaften.**
- Klicken Sie mit der rechten Maustaste auf die Konfigurationsspeichergruppe und klicken Sie dann auf **Eigenschaften.**

In den folgenden Abschnitten werden die speziellen Registerkarten für die Gruppenfamilie erörtert, die im Dialogfeld **Eigenschaften** für die Konfigurationsspeichergruppe enthalten sind.

Registerkarte „Allgemein“

Auf der Registerkarte **Allgemein** wird der Name der Gruppenfamilie angezeigt. Außerdem können Sie hier ihre Beschreibung bearbeiten:

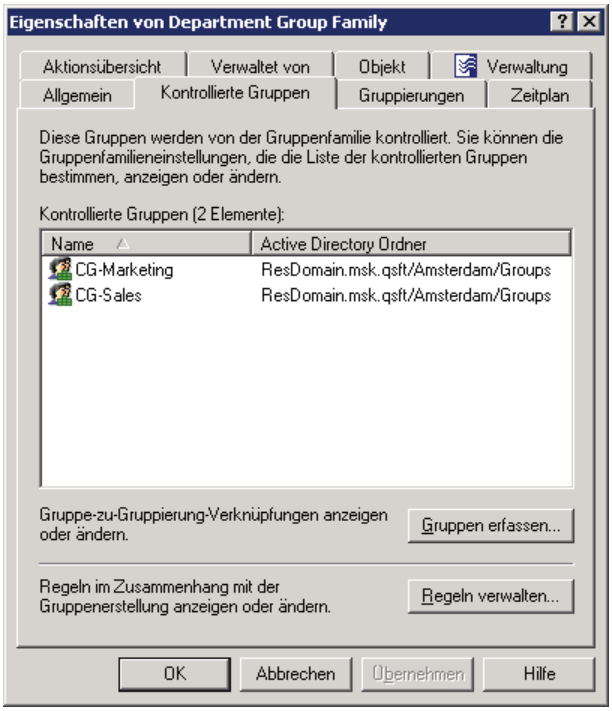


Der Name der Gruppenfamilie kann auf dieser Registerkarte nicht geändert werden. Verwenden Sie zum Ändern des Namens den Befehl **Umbenennen** für die Konfigurationsspeichergruppe.

Indem Sie auf **Speichergruppenbereich und typ (erweitert)** klicken, können Sie den Bereich anzeigen, der zum Anzeigen und Ändern des Gruppenbereichs und des Gruppentyps der Konfigurationsspeichergruppe dient. Änderungen an diesen Einstellungen haben keine Auswirkungen auf die Gruppenfamilie. Der Gruppentyp und der Gruppenbereich sind standardmäßig auf den Sicherheitstyp und den globalen Bereich festgelegt. Normalerweise müssen sie nicht geändert werden.

Registerkarte „Kontrollierte Gruppen“

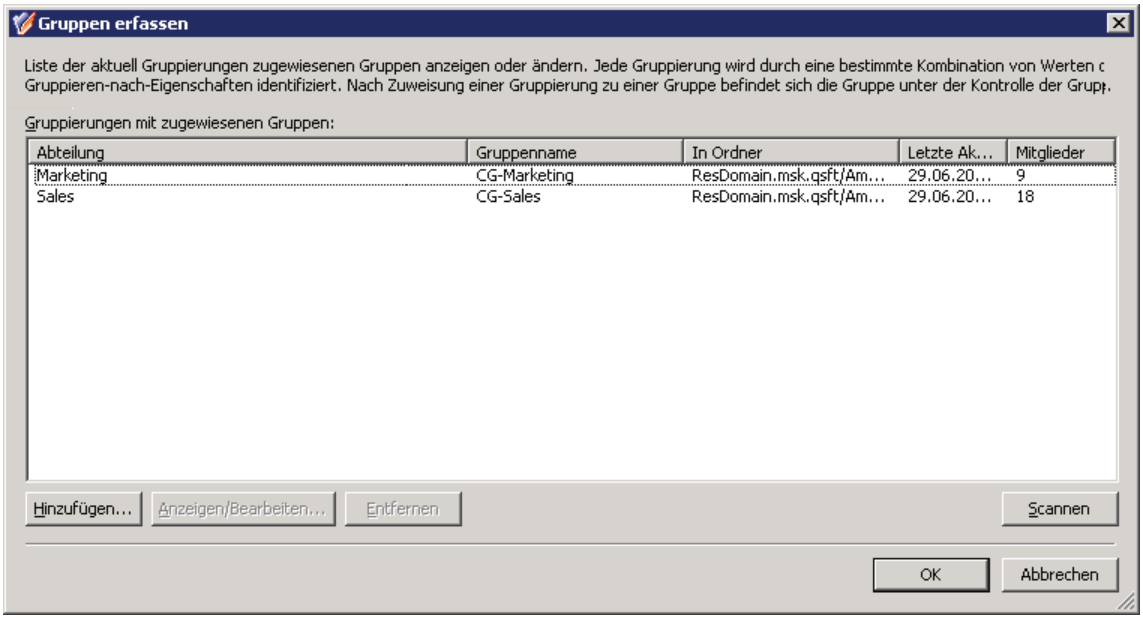
Auf der Registerkarte **Kontrollierte Gruppen** wird eine Liste der Gruppen angezeigt, die von der Gruppenfamilie kontrolliert werden:



Jede der aufgelisteten Gruppen wird von der Gruppenfamilie erstellt oder erfasst und mit einer bestimmten Gruppierung verknüpft. Sie können diese Verknüpfungen anzeigen oder ändern, wenn Sie auf **Gruppen erfassen** klicken.

Für eine neu erstellte Gruppenfamilienkonfiguration schließt die Liste auf dieser Tabelle nur die Gruppen ein, die im Schritt **Vorhandene Gruppen manuell erfassen** des Assistenten „Neue Gruppenfamilie“ angegeben wurde. Wenn dieser Schritt ausgelassen wurde, ist die Liste leer, bis die Gruppenfamilie mindestens einmal ausgeführt wurde.

Wenn Sie auf **Gruppen erfassen** klicken, wird ein Fenster angezeigt, in dem die Liste der kontrollierten Gruppen detaillierter angezeigt wird. Im Fenster **Gruppen erfassen** können Sie Einträge dieser Liste hinzufügen, ändern oder entfernen.



Im Fenster **Gruppen erfassen** werden alle kontrollierten Gruppen aufgelistet. Für jede Gruppe wird angezeigt, welche Gruppierung mit ihr verknüpft ist. Wie immer werden Gruppierungen durch Kombinationen von Werten der Gruppieren-nach-Eigenschaften identifiziert. Jeder Eintrag in der Liste schließt daher die folgenden Informationen ein:

- **Kombination von Werten der „Gruppieren-nach-Eigenschaften".** Die Kombination von Eigenschaftswerten, die eine Gruppierung identifiziert.
- **Gruppenname.** Identifiziert die Gruppe, die mit der Gruppierung verknüpft ist.
- **In Ordner.** Der kanonische Name des Containers, der die Gruppe enthält.
- **Letzte Aktualisierung.** Das Datum und die Uhrzeit der letzten Aktualisierung dieser Gruppe durch die Gruppenfamilie. Die Aktualisierung tritt während einer Ausführung der Gruppenfamilie auf. Dabei werden ggf. alle Änderungen an der Gruppierung erkannt, und die Mitgliedschaftsliste der Gruppe wird so geändert, dass sie diese Änderungen widerspiegelt.
- **Mitglieder.** Die Anzahl der Mitglieder in der Gruppe nach der letzten Aktualisierung. Diese entspricht der Anzahl der Objekte, die die Gruppenfamilie zum Zeitpunkt der letzten Aktualisierung in der Gruppierung gefunden hat.

Im Fenster **Gruppen erfassen** stehen folgende Schaltflächen zum Verwalten der Liste zur Verfügung:

- **Hinzufügen.** Öffnet ein Fenster, in dem Sie eine vorhandene Gruppe auswählen und eine Gruppierung angeben können, mit der die Gruppe verknüpft (ihr zugewiesen) werden soll. Um eine Gruppierung anzugeben, müssen Sie einen bestimmten Wert jeder der Gruppieren-nach-Eigenschaften eingeben. Dann wird die ausgewählte Gruppe mit der Gruppierung verknüpft, die durch die eingegebene Wertekombination identifiziert wird.
- **Bearbeiten.** Ermöglicht das Ändern eines Eintrags, den Sie in der Liste auswählen. Öffnet ein Fenster, in dem Sie eine andere Gruppe auswählen können oder eine andere Gruppierung angeben können, indem Sie die Wertekombination der Gruppieren-nach-Eigenschaften ändern.

- **Entfernen.** Löscht die ausgewählten Einträge aus der Liste. Die Gruppenfamilie erstellt dann neue Gruppen für die Gruppierungen, die Sie aus der Liste entfernt haben.
- **Scannen.** Erkennt neue Kombinationen von Gruppieren-nach-Eigenschaften und zeigt diese in der Liste an, sodass Sie sie mit vorhandenen Gruppen zu einer neuen Kombination verknüpfen können, wenn die Gruppenfamilie nicht neue Gruppen für diese Kombinationen erstellen soll.

Beachten Sie Folgendes bei der Verwaltung der Gruppenliste im Fenster **Gruppen erfassen**:

- Sie können eine vorhandene Gruppe einer Gruppierung unabhängig davon zuweisen, ob die Gruppierung im Verzeichnis tatsächlich vorhanden ist. Sie können beispielsweise eine Gruppe einer Gruppierung mit einem Wert für die Abteilungseigenschaft zuweisen, der im Verzeichnis nicht enthalten ist. Wenn die Abteilungseigenschaft für Benutzer auf diesen Wert festgelegt wird, fügt die Gruppenfamilie diese Benutzer der angegebenen Gruppe hinzu, statt für die neue Abteilung eine neue Gruppe zu erstellen.
- Jeder Gruppierung kann nur eine einzige Gruppe zugewiesen werden. Wenn die Liste eine bestimmte Gruppierung bereits enthält, können Sie keinen neuen Eintrag hinzufügen, der auf dieselbe Gruppierung verweist. In diesem Fall können Sie die Schaltfläche **Bearbeiten** verwenden, um eine andere Gruppe mit der Gruppierung zu verknüpfen.
- Wenn Sie einen Listeneintrag bearbeiten, um eine andere Gruppe mit einer Gruppierung zu verknüpfen, bleibt die zuvor mit der Gruppierung verknüpfte Gruppe unverändert. Sie wird nicht gelöscht, und ihre Mitgliedschaftsliste wird nicht aktualisiert. Die Mitglieder dieser Gruppierung gehören also immer noch zu der Gruppe, obwohl Sie die Gruppe aus der Liste entfernt haben und sie somit nicht mehr von der Gruppenfamilie kontrolliert wird.
- Wenn Sie einen Eintrag aus der Liste entfernen, wird die Gruppe, auf die er verweist, nicht gelöscht. Während einer späteren Ausführung erkennt die Gruppenfamilie eine Gruppierung, der keine Gruppe zugewiesen ist, und versucht, eine Gruppe für sie zu erstellen. Dieser Vorgang kann aufgrund eines Namenskonflikts fehlschlagen, wenn eine Gruppe mit demselben Namen vorhanden ist, also die Gruppe, die zuvor mit der Gruppierung verknüpft war. Um Namenskonflikte zu vermeiden, sollten Sie die Gruppen, die Sie aus der Kontrolle der Gruppenfamilie entfernen, umbenennen oder löschen.

Regeln im Zusammenhang mit der Gruppenerstellung

Wenn eine Gruppenfamilie eine Gruppierung erkennt, die nicht mit einer Gruppe verknüpft ist, erstellt sie eine neue Gruppe, verknüpft die neue Gruppe mit der Gruppierung und fügt ihr Mitglieder der Gruppierung hinzu. Die Gruppenfamilienkonfiguration gibt eine Reihe von Regeln für das Einrichten bestimmter Eigenschaften für neue Gruppen an.

Die Regeln, die den Gruppenerstellungsprozess steuern, werden bei der Erstellung der Gruppenfamilienkonfiguration definiert. Um diese Regeln zu untersuchen oder zu ändern, verwenden Sie im Dialogfeld **Eigenschaften** der Gruppenfamilienkonfigurations-Speichergruppe auf der Registerkarte **Kontrollierte Gruppen** die Schaltfläche **Regeln verwalten**.

Über die Schaltfläche **Regeln verwalten** haben Sie Zugriff auf eine Reihe von Seiten, die denen des Assistenten „Neue Gruppenfamilie" ähneln. Dieser Assistent wird weiter oben in diesem Kapitel diskutiert. Wenn Sie auf **Regeln verwalten** klicken, wird ein schrittweiser Vorgang gestartet, der folgende Seiten umfasst:

- **Gruppenbenennungsregel.** Die Gruppenfamilie verwendet diese Regel bei der Erstellung neuer Gruppen zum Generieren folgender Werte: Gruppenname, Anzeigename, Gruppenname (Prä-Windows 2000) und E-Mail-Alias. Weitere Informationen finden Sie im Abschnitt Gruppenbenennungsregel weiter oben in diesem Kapitel.

- **Gruppenbereich und typ.** Der Gruppentyp und der Gruppenbereich, die den von der Gruppenfamilie erstellten Gruppen zugewiesen werden.
- **Ort der Gruppen.** Die Regel, die bestimmt, in welchem Container die Gruppenfamilie neue Gruppen erstellt. Weitere Informationen finden Sie im Abschnitt Ort der Gruppen weiter oben in diesem Kapitel.
- **Exchange-bezogene Einstellungen.** Die Regel, die bestimmt, ob die von der Gruppenfamilie erstellten Gruppen E-Mail-fähig sind. Außerdem legt diese Regel eine Reihe von Optionen für E-Mail-fähige Gruppen fest. Weitere Informationen finden Sie im Abschnitt Exchange-bezogene Einstellungen weiter oben in diesem Kapitel.

Sie können mit Hilfe der Schaltflächen **Zurück** und **Weiter** durch diese Seiten navigieren. Mit der Schaltfläche **Fertig stellen** auf der letzten Seite werden ggf. die Änderungen von allen Seiten im Dialogfeld **Eigenschaften** festgeschrieben, und die Verwaltungsaufgabe für die Gruppenerstellungsregeln wird abgeschlossen. Die Änderungen werden übernommen, wenn Sie im Dialogfeld **Eigenschaften** auf **OK** oder **Anwenden** klicken. Wenn Sie sie verwerfen möchten, klicken Sie auf **Abbrechen**.

Registerkarte „Gruppierungen“

Über die Registerkarte **Gruppierungen** können Sie auf die Benutzeroberfläche zum Konfigurieren der Gruppenfamilieneinstellungen zugreifen, die den Berechnungsprozess für Gruppierungen steuern.

Während jeder Ausführung berechnet die Gruppenfamilie Gruppierungen neu. Dazu zerlegt sie die Menge der verwalteten Objekte (den Bereich) in Teilmengen. Jede Teilmenge besteht aus den Objekten, für die jeder der Gruppieren-nach-Eigenschaften ein bestimmter Wert zugewiesen ist.

Die Einstellungen, die den Bereich und die Gruppieren-nach-Eigenschaften bestimmen, werden bei der Erstellung der Gruppenfamilienkonfiguration definiert. Sie können diese Einstellungen mit Hilfe der Schaltfläche **Konfigurieren** auf der Registerkarte **Gruppierungen** untersuchen oder ändern.

Über die Schaltfläche **Konfigurieren** haben Sie Zugriff auf eine Reihe von Seiten, die denen des Assistenten „Neue Gruppenfamilie“ ähneln. Dieser Assistent wird weiter oben in diesem Kapitel diskutiert. Wenn Sie auf **Konfigurieren** klicken, wird ein schrittweiser Vorgang gestartet, der folgende Seiten umfasst:

- **Ort der verwalteten Objekte.** Die Verzeichniscontainer, in denen die Gruppenfamilie nach Objekten sucht, die in den Bereich eingeschlossen werden sollen. Weitere Informationen finden Sie im Abschnitt Ort der verwalteten Objekte weiter oben in diesem Kapitel.
- **Auswahl der verwalteten Objekte.** Die Kriterien, mit denen die Gruppenfamilie bestimmt, ob das jeweilige Objekt in den Bereich eingeschlossen werden soll. Weitere Informationen finden Sie im Abschnitt Auswahl der verwalteten Objekte weiter oben in diesem Kapitel.
- **Gruppieren-nach-Eigenschaften.** Die Liste der Eigenschaften, mit denen die Gruppenfamilie Gruppierungen berechnet. Weitere Informationen finden Sie im Abschnitt Gruppieren-nach-Eigenschaften weiter oben in diesem Kapitel.

Sie können mit Hilfe der Schaltflächen **Zurück** und **Weiter** durch diese Seiten navigieren. Mit der Schaltfläche **Fertig stellen** auf der letzten Seite werden ggf. die Änderungen von allen Seiten im Dialogfeld **Eigenschaften** festgeschrieben, und die Verwaltungsaufgabe für die Gruppierungsberechnungsregeln wird abgeschlossen. Die Änderungen werden übernommen, wenn Sie im Dialogfeld **Eigenschaften** auf **OK** oder **Anwenden** klicken. Wenn Sie sie verwerfen möchten, klicken Sie auf **Abbrechen**.

Wenn Sie die Änderungen an der Liste auf der Seite **Gruppieren-nach-Eigenschaften** übernommen haben, legen Sie die Gruppenfamilienoptionen neu fest, die von den Gruppieren-nach-Eigenschaften abhängig sind. Zu diesen Optionen gehören die Gruppenbenennungsregeln und die Liste der zu erfassenden Gruppen. Wenn Sie eine Gruppieren-nach-Eigenschaft hinzufügen oder entfernen, werden die aktuellen Benennungsregeln durch die Standardbenennungsregel ersetzt, und die Liste der zu erfassenden Gruppen wird gelöscht.

Registerkarte „Zeitplan“

Die Registerkarte **Zeitplan** zeigt Informationen zum Zeitplan der Gruppenfamilie an und ermöglicht Ihnen das Anzeigen oder Ändern von Zeitplanungseinstellungen.

Auf der Registerkarte werden die folgenden Informationen angezeigt:

- **Zeitplan.** Für die Gruppenfamilie wird die Ausführung anhand dieser Anweisung geplant.
- **Auf diesem Server ausführen.** Der Verwaltungsdienst, der alle für die Ausführung der Gruppenfamilie notwendigen Vorgänge ausführt.
- **Letzte Laufzeit.** Das Datum und die Uhrzeit der letzten Ausführung der Gruppenfamilie.
- **Nächste Ausführungszeit.** Das Datum und die Uhrzeit der geplanten nächsten Ausführung der Gruppenfamilie.

Über die Schaltfläche **Konfigurieren** können Sie den Zeitplan der Gruppenfamilie detaillierter untersuchen und ihn nach Bedarf anpassen.

Durch Anklicken von **Konfigurieren** wird die Seite **Planung für Gruppenfamilie** angezeigt, die mit der weiter oben in diesem Kapitel beschriebenen Seite des Assistenten zur Erstellung einer neuen Gruppenfamilie identisch ist (siehe Abschnitt Planung für Gruppenfamilie). Betrachten oder ändern Sie die Zeitplaneinstellungen auf dieser Seite und klicken Sie auf die Schaltfläche **Fertig stellen**, um Ihre Änderungen im Dialogfeld **Eigenschaften** festzuschreiben. Die Änderungen werden übernommen, wenn Sie auf die Schaltfläche **OK** oder **Anwenden** klicken. Wenn Sie sie verwerfen möchten, klicken Sie auf **Abbrechen**.

Registerkarte „Vorgangsübersicht“

Auf der Registerkarte **Vorgangsübersicht** werden quantitative Informationen zur Ausführung der Gruppenfamilie angezeigt.

Auf der Registerkarte **Vorgangsübersicht** werden folgende Informationen zur letzten Ausführung der Gruppenfamilie angezeigt:

- **Letzte Ausführung gestartet.** Das Datum und die Uhrzeit des Ausführungsstarts.
- **Letzte Ausführung beendet.** Das Datum und die Uhrzeit des Ausführungsendes.
- **Verwaltete Objekte.** Die Anzahl der Objekte, die im Bereich der Gruppenfamilie gefunden wurden.

- **Gültige Gruppierungen.** Die Anzahl der Gruppierungen, die während der Ausführung berechnet wurden.
- **Fehlerhafte Gruppierungen.** Die Anzahl der Gruppierungen, die die Gruppenfamilie nicht identifizieren konnte, weil ihre Gruppieren-nach-Eigenschaften ungültige Wertekombinationen aufweisen. Beispielsweise tritt eine ungültige Kombination auf, wenn Werte für mindestens eine Eigenschaft in der Kombination fehlen.
- **Erstellte Gruppen.** Die Anzahl der Gruppen, die die Gruppenfamilie während der Ausführung erstellt hat.
- **Aktualisierte Gruppen.** Die Anzahl der Gruppen, für die die Gruppenfamilie während der Ausführung die Mitgliedschaftslisten aktualisiert hat.
- **Aktualisierungen in Gruppenmitgliedschaften.** Die Anzahl der Objekte, die die Gruppenfamilie während der Ausführung zu Gruppen hinzugefügt oder aus Gruppen entfernt hat.
- **Fehler.** Die Anzahl der Fehler während der Ausführung.

Um diese Informationen genauer zu untersuchen, klicken Sie auf die Schaltfläche **Protokoll anzeigen**.

Aktions-Übersichtsprotokoll

Wenn Sie auf die Schaltfläche **Protokoll anzeigen** klicken, wird ein Protokoll mit Zusammenfassungsinformationen zur letzten Ausführung der Gruppenfamilie angezeigt. Das Protokoll enthält ggf. Beschreibungen der Fehlersituationen, die während der Ausführung aufgetreten sind, und fasst die quantitativen Ergebnisse der Ausführung zusammen, z.B. die Anzahl aktualisierter Gruppen, die Anzahl erstellter Gruppen und die Anzahl der Objekte, deren Gruppenmitgliedschaften geändert wurden.

Das Protokoll besteht aus drei Abschnitten: Prolog, Fehlerliste und Epilog. Die Abschnitte „Prolog" und „Epilog" sind immer im Protokoll enthalten. Dagegen ist die „Fehler Liste" nur dann vorhanden, wenn bei der Ausführung Fehler oder Warnungen aufgetreten sind.

Der Abschnitt „Prolog" bietet die folgenden Informationen:

- Das Datum und die Uhrzeit des Ausführungsstarts
- Die Anzahl der verwalteten Objekte, die im Bereich der Gruppenfamilie gefunden wurden
- Die Gesamtanzahl der Gruppierungen, die durch Analyse der Gruppieren-nach-Eigenschaften gefunden wurden

Der Abschnitt „Epilog" bietet die folgenden Informationen:

- Ggf. die Anzahl der Fehler
- Ggf. die Anzahl ungültiger Wertekombinationen von Gruppieren-nach-Eigenschaften
- Die Anzahl der Gruppen, die die Gruppenfamilie während der Ausführung erstellt hat
- Die Anzahl der Gruppen, die die Gruppenfamilie während der Ausführung aktualisiert hat

Der Fehler Liste enthält Informationen zu allen Fehlern und Warnungen, die während der Ausführung der Gruppenfamilie aufgetreten sind.

Zusammenfassung: Verfahren zur Verwaltung einer Gruppenfamilie

Dieses Hilfethema deckt einige aufgabenspezifische Verfahren ab, die Sie verwenden können, um die Konfiguration und Eigenschaften einer vorhandenen Gruppenfamilie zu ändern.

Gehen Sie folgendermaßen vor die Eigenschaftsmaske einer Gruppenfamilie zu öffnen:

- Klicken Sie mit der rechten Maustaste auf die Gruppenfamilien-Konfigurationsspeichergruppe und klicken Sie dann auf **Eigenschaften**.

Gehen Sie folgendermaßen vor, um Gruppierungsregeln anzuzeigen oder zu ändern:

1. Öffnen Sie die Eigenschaftenseite für die Gruppenfamilie (siehe Anleitungen weiter oben in diesem Hilfethema).
2. Klicken Sie auf die Registerkarte **Gruppierungen** und dann auf **Konfigurieren**.
3. Befolgen Sie die Schritte 5 bis 7 des Verfahrens zur Erstellung einer Gruppenfamilie (siehe Zusammenfassung: Verfahren zur Erstellung einer Gruppenfamilie).
4. Klicken Sie auf der Seite **Gruppieren-nach Eigenschaft** auf **Fertig stellen**.
5. Klicken Sie auf **OK**, um die Eigenschaftenseite zu schließen.

Gehen Sie folgendermaßen vor, um erstellungsrelevante Regeln anzuzeigen oder zu ändern:

1. Öffnen Sie die Eigenschaftenseite für die Gruppenfamilie (siehe Anleitungen weiter oben in diesem Hilfethema).
2. Klicken Sie auf die Registerkarte **Kontrollierte Gruppen** und dann auf **Regeln verwalten**.
3. Befolgen Sie die Schritte 9 bis 12 des Verfahrens zur Erstellung einer Gruppenfamilie (siehe Zusammenfassung: Verfahren zur Erstellung einer Gruppenfamilie).
4. Klicken Sie auf der Seite **Exchange-bezogene Einstellungen** auf **Fertig stellen**.
5. Klicken Sie auf **OK**, um die Eigenschaftenseite zu schließen.

Gehen Sie folgendermaßen vor, um eine Gruppe manuell zu einer Gruppenfamilie hinzuzufügen:

1. Öffnen Sie die Eigenschaftenseite für die Gruppenfamilie (siehe Anleitungen weiter oben in diesem Hilfethema).
2. Klicken Sie auf die Registerkarte **Kontrollierte Gruppen** und dann auf **Gruppen erfassen**.
3. Klicken Sie im Fenster **Gruppen erfassen** auf **Hinzufügen**.
4. Nehmen Sie im Dialogfeld **Gruppe zu Gruppierung zuweisen** Folgendes vor und klicken Sie auf **OK**:
   a) Klicken Sie auf **Wählen** und wählen Sie dann die Gruppe aus, die Sie hinzuzufügen möchten.
   b) Geben Sie unter **Gruppieren-nach Eigenschaft** einen Wert für die Gruppieren-nach Eigenschaft ein. Wenn mehrere Gruppieren-nach Eigenschaften definiert sind, geben Sie einen Wert für jede Eigenschaft ein, um die Gruppierung festzulegen, der Sie die Gruppe zuordnen möchten.
5. Klicken Sie auf **OK**, um das Fenster **Gruppen erfassen** zu schließen.
6. Klicken Sie auf **OK**, um die Eigenschaftenseite zu schließen.

Gehen Sie folgendermaßen vor, um eine Gruppe aus einer Gruppenfamilie zu entfernen:

1. Öffnen Sie die Eigenschaftenseite für die Gruppenfamilie (siehe Anleitungen weiter oben in diesem Hilfethema).
2. Klicken Sie auf die Registerkarte **Kontrollierte Gruppen** und dann auf **Gruppen erfassen**.

3. Wählen Sie im Fenster **Gruppen erfasse**n die Gruppe aus, die Sie aus der Gruppenfamilie entfernen möchten, klicken Sie dann auf **Entfernen** und klicken Sie dann auf **OK**.
4. Klicken Sie auf **OK**, um die Eigenschaftenseite zu schließen.

Gehen Sie folgendermaßen vor, um eine Gruppenfamilienaktualisierung zu planen:

1. Öffnen Sie die Eigenschaftenseite für die Gruppenfamilie (siehe Anleitungen weiter oben in diesem Hilfethema).
2. Klicken Sie auf die Registerkarte **Zeitplan** und dann auf **Konfigurieren**.
3. Gehen Sie auf der Seite **Planung für Gruppenfamilie** wie nachfolgend beschrieben vor und klicken Sie dann auf **Fertig stellen**:
   a) Wählen Sie **Ausführung der Gruppenfamilie planen** aus und legen Sie dann das entsprechende Datum, die entsprechende Uhrzeit und die Frequenz der Gruppenfamilienaktualisierung fest.
   b) Wenn Sie außerdem möchten, dass die Gruppenfamilie sofort nach dem Schließen der Eigenschaftenseite einmalig ausgeführt wird, wählen Sie **Gruppenfamilie einmalig ausführen, nachdem diese Seite ausgefüllt wurde**.
   c) Wählen Sie in der Liste **Auf diesem Server ausführen** den Verwaltungsdienst aus, der die Gruppenfamilie ausführen soll.
4. Klicken Sie auf **OK**, um die Eigenschaftenseite zu schließen.

Gehen Sie folgendermaßen vor, um die Ergebnisse einer Gruppenfamilienaktualisierung anzuzeigen:

1. Öffnen Sie die Eigenschaftenseite für die Gruppenfamilie (siehe Anleitungen weiter oben in diesem Hilfethema).
2. Klicken Sie auf die Registerkarte **Aktionsübersicht** und dann auf **Protokoll anzeigen**.

Gehen Sie folgendermaßen vor, um eine Gruppenfamilie zu löschen:

- Klicken Sie mit der rechten Maustaste auf die Gruppenfamilien-Konfigurationsspeichergruppe und klicken Sie dann auf **Löschen**.

Durch das Löschen einer Gruppenfamilie wird nur die Konfigurationsspeichergruppe der Gruppenfamilie gelöscht. Dieser Vorgang löscht nicht die kontrollierten Gruppen der Gruppenfamilie. Zu einem späteren Zeitpunkt können Sie eine andere Gruppenfamilie konfigurieren, die die Kontrolle über diese Gruppen übernimmt.

Szenario: Abteilungsbezogene Gruppenfamilie

Um die Ausführung der Gruppenfamilienfunktionen zu sehen, können Sie das folgende Szenario durchlaufen.

Angenommen, die Organisationseinheit (Organizational Unit, OU) für Benutzer enthält eine Reihe von Benutzerkonten. Nehmen Sie außerdem an, dass sich für jeden der unten aufgelisteten Werte mindestens ein Konto in der Organisationseinheit für Benutzer befindet, das diesen Wert als Abteilungseigenschaft aufweist. Die folgenden Werte der Abteilungseigenschaft finden sich für die Benutzerkonten in der Organisationseinheit für die Benutzer:

- Accounting (Buchhaltung)
- Educational Services (Bildung)
- Executive Services (Personaldienstleistungen)
- Facilities (Versorgungsaufgaben)
- Finance (Finanzen)
- Government Services (behördliche Dienste)

- Human Resources (Personalabteilung)
- Information Technology (IT)
- International Services (internationale Dienstleistungen)
- Vorgänge

In diesem Abschnitt finden Sie Anweisungen zum Implementieren einer Gruppenfamilie, die für die Benutzer in jeder diese Abteilungen eine eigene Gruppe erstellt und pflegt. Die Gruppenfamilien-Konfigurationsspeichergruppe wird in der Organisationseinheit für Gruppen erstellt. Die Gruppenfamilie wird so konfiguriert, dass sie die Abteilungsgruppen in derselben Organisationseinheit erstellt.

Öffnen Sie die Quest One ActiveRoles-Konsole, und führen Sie die folgenden Schritte aus, um die Gruppenfamilie zu implementieren.

So erstellen Sie die abteilungsbezogene Gruppenfamilie und führen sie aus:

1. Klicken Sie mit der rechten Maustaste auf die Organisationseinheit **Groups** und klicken Sie dann auf **Neu | Gruppenfamilie**.

   Hierdurch wird der Assistent „Neue Gruppenfamilie" gestartet. Die übrigen Schritte gelten für diesen Assistenten.
2. Klicken Sie auf der Seite „Willkommen" auf **Weiter**.
3. Geben Sie in das Feld **Name der Gruppenfamilie** den Wert **Abteilungsbezogene Gruppenfamilie** ein. Klicken Sie auf **Weiter**.
4. Klicken Sie auf die Option **Vorkonfigurierte Gruppierung nach**, klicken Sie in der Liste unter dieser Option auf **Department** und klicken Sie dann auf **Weiter**.
5. Entfernen Sie die Organisationseinheit **Gruppen** aus der Liste **Container**, und fügen Sie der Liste die Organisationseinheit **Benutzer** hinzu. Klicken Sie auf **Weiter**.
6. Klicken Sie auf die Option **Benutzer** und dann auf **Weiter**.
7. Stellen Sie sicher, dass die Liste **Nach diese Eigenschaften gruppieren** nur einen Eintrag enthält, nämlich **Department**. Klicken Sie auf **Weiter**.
8. Aktivieren Sie das Kontrollkästchen **Diesen Schritt ohne manuelle Gruppenerfassung überspringen**. Klicken Sie auf **Weiter**.
9. Klicken Sie auf **Weiter**, um die Standardregel für die Gruppenbenennung zu akzeptieren: **CG-%<Schlüssel.Abteilung.>**
10. Klicken Sie auf **Weiter**, um den Standardbereich und den Standardtyp für die Gruppe zu akzeptieren.
11. Klicken Sie auf **Weiter**, um den Standardspeicherort für die kontrollierten Gruppen zu akzeptieren: **Stammorganisationseinheit der Gruppenfamilie**
12. Klicken Sie auf **Weiter**, um die Standardeinstellungen in Bezug auf Exchange zu akzeptieren.
13. Aktivieren Sie das Kontrollkästchen **Gruppenfamilie einmalig ausführen, nachdem diese Seite ausgefüllt wurde**. Klicken Sie auf **Weiter**.
14. Klicken Sie auf **Fertig stellen**.

Nachdem Sie diese Schritte abgeschlossen haben, führt die Gruppenfamilie die gesamte notwendige Verarbeitung zur Erstellung der Gruppen aus, eine Gruppe pro Abteilung, und fügt Benutzer anhand ihrer Abteilungseigenschaft den entsprechenden Gruppen hinzu.

Sie können sich den Inhalt der Organisationseinheit für **Gruppen** in der Quest One ActiveRoles-Konsole ansehen, um zu überprüfen, ob die Abteilungsgruppen erfolgreich erstellt wurden. Sie können auch Eigenschaften einer von der Gruppenfamilie generierten Gruppe untersuchen, um zu überprüfen, ob die Mitgliedschaftsliste der Gruppe richtig ist. Beispielsweise besteht die Mitgliedschaftsliste der Gruppe **CG-Executive Services (Personaldienstleistungen)** aus den Benutzerkonten, für die die Eigenschaft **Department** auf **Executive Services (Personaldienstleistungen)** festgelegt ist.

9

Dynamische Gruppen

- Grundlegendes zu dynamischen Gruppen
- Richtlinie zu dynamischen Gruppen
- Verwalten dynamischer Gruppen
- Szenario: Automatisches Verschieben von Benutzern zwischen Gruppen

Grundlegendes zu dynamischen Gruppen

In Active Directory können Gruppen (hier als Standardgruppen bezeichnet) Mitglieder statisch enthalten. Quest One ActiveRoles Sie können also Objekte auswählen und sie den Gruppen hinzufügen. Nachdem dieser Prozess eingerichtet ist, fügt er automatisch Mitglieder zu Gruppen hinzu und entfernt sie daraus.

Quest One ActiveRoles stellt regelorientierte Gruppen bereit, die als dynamische Gruppen bezeichnet werden. Mitgliedschaftsregeln bestimmen, ob ein Objekt Mitglied einer dynamischen Gruppe ist. Eine Mitgliedschaftsregel kann die Form einer Suchabfrage, einer Regel für die statische Einschließung und Ausschließung von Objekten sowie einer Regel für die Einschließung und Ausschließung von Gruppenmitgliedern haben. Wenn die Umgebung verändert wird, werden die Mitgliedschaften von Objekten in dynamischen Gruppen automatisch geändert, um an die neue Umgebung angepasst zu werden.

Dynamische Gruppen von Quest One ActiveRoles reduzieren die Kosten für die Pflege von Listen und Gruppen und erhöhen zugleich die Genauigkeit und Zuverlässigkeit dieser Pflege. Außerdem werden Verteilerlisten und Sicherheitsgruppen automatisch aktuell gehalten, sodass Mitglieder nicht manuell hinzugefügt und entfernt werden müssen.

Um die Pflege von Gruppenmitgliedschaftslisten zu automatisieren, stellen dynamische Gruppen die folgenden Funktionen bereit:

- Regelorientierte Mechanismen, die automatisch Objekte zu Gruppen hinzufügen und aus ihnen entfernen, wenn Objektattribute in Active Directory geändert werden.
- Flexible Mitgliedschaftskriterien, die sowohl das abfragebasierte als auch das statische Füllen von Gruppen ermöglichen.

Auf der Quest One ActiveRoles-Konsole werden dynamische Gruppen mit dem folgenden Symbol markiert:

Wenn Sie eine Standardgruppe in eine dynamische Gruppe konvertieren, verliert die Gruppe alle Mitglieder, die zur Gruppe hinzugefügt worden sind, als diese noch eine Standardgruppe war. Der Grund ist, dass Mitglieder einer dynamischen Gruppe nur über Mitgliedschaftsregeln definiert werden können.

Wenn Sie eine dynamische Gruppe in eine Standardgruppe konvertieren, behält die Gruppe alle ihre Mitglieder, die aufgrund der Mitgliedschaftsregeln in sie eingeschlossen sind, verliert jedoch die Mitgliedschaftsregeln.

Wenn ein Mitglied einer dynamischen Gruppe wie etwa einer Benutzer- oder anderen Gruppe deprovisioniert ist, wird die dynamische Gruppe automatisch so aktualisiert, dass sie dieses Mitglied nicht mehr enthält. Folglich werden bei der Deprovisionierung eines Benutzers oder einer Gruppe dieser Benutzer oder diese Gruppe aus allen dynamischen Gruppen entfernt. Dieses Verhalten ist Absicht.

Richtlinie zu dynamischen Gruppen

Das Verhalten des Mechanismus für dynamische Gruppen wird von der Richtlinie definiert, die im integrierten Richtlinienobjekt „dynamische Gruppen" definiert ist. Mit dieser Richtlinie wird sichergestellt, dass alle mit einem beliebigen anderen Active Directory-Verwaltungstool an einer dynamischen Gruppe vorgenommenen Änderungen verworfen werden. Mitgliedschaftslisten können nur mit den Mitgliedschaftsregeln von Quest One ActiveRoles geändert werden.

Um die Richtlinie anzuzeigen oder zu ändern, zeigen Sie das Dialogfeld **Eigenschaften** für das Richtlinienobjekt **Built-in Policy – Dynamic Groups** an (dies befindet sich im Container **Configuration/Policies/Administration/Builtin**), öffnen Sie die Registerkarte **Richtlinien**, wählen Sie die Richtlinie aus und klicken Sie auf **Anzeigen/Bearbeiten**. Nun wird das Dialogfeld **Richtlinieneigenschaften** angezeigt.

Auf der Registerkarte **Richtlinieneinstellungen** des Dialogfelds **Richtlinieneigenschaften** können Sie die folgenden Optionen einrichten:

- **Maximale Anzahl von Mitgliedern pro Gruppe.** Gibt die maximal zulässige Anzahl von Mitgliedern einer dynamischen Gruppe an. Wenn die Mitgliedschaftsliste einer dynamischen Gruppe diesen Grenzwert überschreitet, erstellt Quest One ActiveRoles zusätzliche Gruppen, um die verbleibenden Mitglieder aufzunehmen, und fügt diese Gruppen zur dynamischen Gruppe hinzu.

  Wenn Quest One ActiveRoles keine verschachtelten Gruppen erstellen soll, deaktivieren Sie das Kontrollkästchen **Verschachtelte Gruppen erstellen, um zusätzliche Mitglieder aufzunehmen**. Wenn dieses Kontrollkästchen deaktiviert ist, ermöglicht die Richtlinie, dass dynamische Gruppen jede beliebige Anzahl von Mitgliedern enthalten können.

  Für dynamische Gruppen in Domänen, deren Gesamtstruktur-Funktionsebene auf Windows Server 2003 oder höher gesetzt ist, werden keine verschachtelten Gruppen erstellt. In diesem Fall ermöglicht die Richtlinie unabhängig vom Status des Kontrollkästchens, dass eine dynamische Gruppe jede beliebige Anzahl von Mitgliedern enthält.

- **Verzeichnisänderungen von DirSync-Steuerung empfangen.** Stellt sicher, dass die Richtlinie unabhängig davon, welche Tools für die Verwaltung von Active Directory verwendet werden, die Mitgliedschaftslisten richtig auffüllt. Wenn dieses Kontrollkästchen nicht aktiviert ist, sind einige regelorientierte Mitgliedschaftslisten möglicherweise mit Mitgliedschaftsregeln inkompatibel. In diesem Fall wendet die Richtlinie Mitgliedschaftsregeln nur dann neu an, wenn mit Quest One ActiveRoles Änderungen am Verzeichnis vorgenommen werden.
- **Nur Mail-aktivierte Benutzer in dynamische Verteilergruppen einschließen.** Verhindert, dass die Richtlinie Benutzer ohne Exchange-Postfach zu Verteilergruppen hinzufügt, die als dynamische Gruppen konfiguriert sind.
- **Fügen Sie diese Nachricht für die einzelnen dynamischen Gruppen im Feld „Hinweise" hinzu.** Legt den Nachrichtentext in der Eigenschaft **Hinweise** jeder dynamischen Gruppe ab. (Die Eigenschaft **Hinweise** wird im Dialogfeld **Eigenschaften** für die Gruppe auf der Registerkarte **Allgemein** angezeigt).

Verwalten dynamischer Gruppen

In diesem Abschnitt wird die Administration dynamischer Gruppen mit der Quest One ActiveRoles-Konsole vorgestellt. Folgende Themen werden erörtert:

- Konvertieren einer Standardgruppe in eine dynamische Gruppe
- Anzeigen der Mitglieder einer dynamischen Gruppe
- Hinzufügen einer Mitgliedschaftsregel zu einer dynamischen Gruppe
- Entfernen einer Mitgliedschaftsregel aus einer dynamischen Gruppe
- Konvertieren einer dynamischen Gruppe in eine Standardgruppe
- Ändern, Umbenennen oder Löschen einer dynamischen Gruppe

Konvertieren einer Standardgruppe in eine dynamische Gruppe

Klicken Sie zum Konvertieren einer Standardgruppe in eine dynamische Gruppe mit der rechten Maustaste auf die Gruppe und klicken Sie dann auf **In dynamische Gruppe konvertieren**, um den Assistenten für neue Mitgliedschaftsregel zu starten. Die erste Seite des Assistenten entspricht der folgenden Abbildung.

Assistent für neue Mitgliedschaftsregel
Typ der Mitgliedschaftsregel wählen:
Regeltyp
Beschreibung
Explizit einschließen
Objekts statisch einschließen
Nach Abfrage einschli...
Von Abfrage zurückgegebene Objekte einschli...
Gruppenmitglieder ein...
Mitglieder gewählter Gruppen einschließen
Explizit ausschließen
Objekte statisch ausschließen
Nach Abfrage ausschl...
Von Abfrage zurückgegebene Objekte ausschli...
Gruppenmitglieder au...
Mitglieder gewählter Gruppen ausschließen
Beschreibung der Mitgliedschaftsregel:
Objekte zum Hinzufügen zur Mitgliedschaftsliste wählen.
ActiveRoles Server stellt sicher, dass die gewählten Objekte in der Mitgliedschaftsliste enthalten sind, unabhängig davon, ob sie umbenannt, in einen anderen Container verschoben oder ihre Eigenschaften geändert
< Zurück
Weiter >
Abbrechen
Hilfe

Auf der ersten Seite des Assistenten können Sie den Typ der zu konfigurierenden Mitgliedschaftsregel auswählen. Im Text unter **Beschreibung der Mitgliedschaftsregel** wird erläutert, welche Mitgliedschaftsregeln mit dem ausgewählten Regeltyp erstellt werden können.

Die Mitgliedschaftsregel **Explizit einschließen** ermöglicht das Auswählen von Objekten, die der Gruppe statisch hinzugefügt werden. Quest One ActiveRoles stellt sicher, dass die gewählten Objekte immer in die Gruppe aufgenommen werden, auch wenn sie umbenannt, in einen anderen Behälter verschoben oder mit geänderten Eigenschaften versehen wurden. Mit dem Regeltyp **Explizit einschließen** verhält sich die dynamische Gruppe wie eine Standardgruppe.

Die Mitgliedschaftsregel **Durch Abfrage einschließen** ermöglicht das Definieren von Kriterien, die Objekte zur Aufnahme in die Gruppe erfüllen müssen. Quest One ActiveRoles befüllt die Mitgliedschaftsliste der Gruppe dynamisch mit den Objekten, die bestimmte Eigenschaften aufweisen. Wenn ein Objekt erstellt wird oder wenn seine Eigenschaften geändert werden, fügt Quest One ActiveRoles dieses Objekt der Gruppe hinzu bzw. entfernt es daraus, abhängig davon, ob die Eigenschaften des Objekts den definierten Kriterien entsprechen.

Die Mitgliedschaftsregel **Gruppenmitglieder einschließen** ermöglicht das Auswählen der Gruppen, deren Mitglieder Sie in die dynamische Gruppe aufnehmen möchten. Quest One ActiveRoles befüllt die Gruppen-Mitgliedschaftsliste dynamisch mit den Objekten, die zu den ausgewählten Gruppen gehören. Wenn ein Objekt den ausgewählten Gruppen hinzugefügt oder aus ihnen entfernt wird, fügt Quest One ActiveRoles dieses Objekt der dynamischen Gruppe hinzu bzw. entfernt es aus ihr.

Die Mitgliedschaftsregel **Explizit ausschließen** ermöglicht das Auswählen von Objekten, die statisch aus der Gruppe ausgeschlossen werden. Quest One ActiveRoles stellt sicher, dass die gewählten Objekte immer aus der Gruppe ausgeschlossen werden, auch wenn sie umbenannt, in einen anderen Behälter verschoben oder mit geänderten Eigenschaften versehen wurden. Da die Regel **Explizit ausschließen** Vorrang vor allen anderen Regeltypen hat, werden die ausgewählten Objekte auch dann aus der Gruppe ausgeschlossen, wenn eine andere Regel besagt, dass sie eingeschlossen werden sollen.

Die Mitgliedschaftsregel **Ausschließen nach Abfrage** ermöglicht das Definieren von Kriterien, die Objekte erfüllen müssen, um aus der Gruppe ausgeschlossen zu werden. Quest One ActiveRoles stellt sicher, dass die Objekte mit bestimmten Eigenschaften aus der Gruppen-Mitgliedschaftsliste ausgeschlossen werden. Quest One ActiveRoles entfernt Objekte automatisch aus der Gruppe, unabhängig davon, on deren Eigenschaften den definierten Kriterien entsprechen.

Die Mitgliedschaftsregel **Gruppenmitglieder ausschließen** ermöglicht das Auswählen von Gruppen, deren Mitglieder aus der gegebenen Gruppe ausgeschlossen werden. Quest One ActiveRoles stellt sicher, dass die Mitglieder der gewählten Gruppen aus der Gruppen-Mitgliedschaftsliste ausgeschlossen werden. Wenn ein Objekt einer der ausgewählten Gruppen hinzugefügt wird, entfernt Quest One ActiveRoles dieses Objekt automatisch aus der dynamischen Gruppe.

Wählen Sie auf der ersten Seite des Assistenten einen Regeltyp aus und klicken Sie dann auf **Weiter**. Klicken Sie auf der nächsten Seite des Assistenten auf **Hinzufügen**, um die Mitgliedschaftsregel zu konfigurieren.

Wenn Sie den Regeltyp **Explizit einschließen** oder **Explizit ausschließen** ausgewählt, haben, wird das Dialogfeld **Objekte auswählen** angezeigt, in dem Benutzer, Gruppen, Kontakte und Computer aufgelistet werden. Wählen Sie die Objekte aus, die Sie in die dynamische Gruppe einschließen oder aus ihr ausschließen möchten, klicken Sie auf **Hinzufügen** und dann auf **OK**.

Wenn Sie den Regeltyp **Gruppenmitglieder einschließen** oder **Gruppenmitglieder ausschließen** ausgewählt haben, wird das Dialogfeld **Objekte auswählen** angezeigt. Die Liste der Objekte in diesem Dialogfeld besteht aus Gruppen. Wählen Sie Gruppen aus, klicken Sie auf **Hinzufügen** und dann auf **OK**. Alle Mitglieder der ausgewählten Gruppen werden in die dynamische Gruppe eingeschlossen oder aus ihr ausgeschlossen.

Wenn Sie den Regeltyp **Nach Abfrage einschließen** oder **Nach Abfrage ausschließen** ausgewählt haben, wird das Dialogfeld **Mitgliedschaftsregel erstellen** angezeigt, das dem Dialogfeld **Suchen** ähnelt. Definieren Sie in diesem Dialogfeld die Kriterien, die Objekte erfüllen müssen, um in die dynamische Gruppe eingeschlossen oder aus ihr ausgeschlossen zu werden.

Klicken Sie auf **Fertig stellen**, um den Assistenten „Neue Mitgliedschaftsregel" abzuschließen.

Nachdem Sie eine dynamische Gruppe erstellt und ihr dabei die erste Regel hinzugefügt haben, können Sie weitere Regeln hinzufügen. Verwenden Sie dazu die Verwaltungsfunktionen für Eigenschaften der Gruppe.

Wenn Sie mehrere Mitgliedschaftsregeln hinzufügen und einige davon miteinander in Konflikt stehen, wird der Konflikt durch eine Regel gelöst, die die folgende Rangordnung definiert:

1. Explizit ausschließen
2. Explizit einschließen
3. Nach Abfrage ausschließen
4. Gruppenmitglieder ausschließen
5. Nach Abfrage einschließen
6. Gruppenmitglieder einschließen

Nach dieser Rangfolge hat z.B. die Regel **Explizit ausschließen** Vorrang vor allen anderen Regeltypen. Daher werden die ausgewählten Objekte auch dann aus der dynamischen Gruppe ausgeschlossen, wenn eine andere Regel angibt, dass sie eingeschlossen werden sollen (beispielsweise die Objekte, die die in der Mitgliedschaftsregel **Nach Abfrage einschließen** definierten Kriterien erfüllen, oder Mitglieder eine Gruppe, die in der Regel **Gruppenmitglieder einschließen** ausgewählt wurden).

Anzeigen der Mitglieder einer dynamischen Gruppe

Für eine dynamische Gruppe wird dem Dialogfeld **Eigenschaften** die Registerkarte **Mitgliedschaftsregeln** hinzugefügt. Auf dieser Registerkarte wird eine Liste von Mitgliedschaftsregeln angezeigt, die für die Gruppe definiert sind. Außerdem können Sie hier die Regeln hinzufügen, entfernen und bearbeiten.

Auf der Registerkarte **Mitglieder** für eine dynamische Gruppe wird eine Liste von Objekten angezeigt, die den in den Mitgliedschaftsregeln angegebenen Kriterien entsprechen. Auf dieser Registerkarte können Sie Mitglieder nicht wie bei einer Standardgruppe hinzufügen oder entfernen. Um bestimmte Mitglieder einer dynamischen Gruppe hinzuzufügen oder zu entfernen, können Sie eine entsprechende Mitgliedschaftsregel der Art **Explizit einschließen** oder **Explizit ausschließen** hinzufügen.

Hinzufügen einer Mitgliedschaftsregel zu einer dynamischen Gruppe

Um eine Mitgliedschaftsregel zu einer dynamischen Gruppe hinzuzufügen, klicken Sie mit der rechten Maustaste auf die dynamische Gruppe und klicken Sie dann auf **Mitgliedschaftsregel hinzufügen**. Hierdurch wird der Assistent „Neue Mitgliedschaftsregel" gestartet. Schließen Sie den Assistenten wie unter „Konvertieren einer Standardgruppe in eine dynamische Gruppe" weiter oben in diesem Kapitel beschrieben ab. Um einer dynamischen Gruppe eine Mitgliedschaftsregel hinzuzufügen, können Sie auch die Registerkarte **Mitgliedschaftsregeln** im Dialogfeld **Eigenschaften** verwenden.

So fügen Sie eine Mitgliedschaftsregel zu einer Gruppe hinzu:

1. Wählen Sie in der Konsolenstruktur den Ordner aus, der die Gruppe enthält, zu der Sie eine Mitgliedschaftsregel hinzufügen möchten.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf die Gruppe und führen Sie einen der folgenden Schritte durch, um den Assistenten zum Erstellen einer neuen Mitgliedschaftsregel zu starten:
   - Wenn die Gruppe eine Standardgruppe ist, klicken Sie auf **In dynamische Gruppe konvertieren** und dann auf **Ja**.
   - Wenn die Gruppe eine dynamische Gruppe ist, klicken Sie auf **Mitgliedschaftsregel hinzufügen**.
3. Wählen Sie auf der ersten Seite des Assistenten den Typ der Mitgliedschaftsregel aus, die Sie erstellen möchten. Führen Sie einen der nachfolgend aufgeführten Schritte durch und klicken Sie dann auf **Weiter**:
   - Um eine Regel zu erstellen, die statisch Mitglieder zur Gruppe hinzufügt, klicken Sie auf **Explizit einschließen**.
   - Um eine Regel zu erstellen, die statisch Mitglieder aus der Gruppe ausschließt, klicken Sie auf **Explizit ausschließen**.
   - Um eine Regel zu erstellen, die alle Mitglieder einer bestimmten Gruppe zur ausgewählten Gruppe hinzufügt, klicken Sie auf **Gruppenmitglieder einschließen**.
   - Um eine Regel zu erstellen, die alle Mitglieder einer bestimmten Gruppe aus der ausgewählten Gruppe ausschließt, klicken Sie auf **Gruppenmitglieder ausschließen**.
   - Um eine Regel zu erstellen, die die Gruppe mit den Objekten füllt, die bestimmte Suchkriterien erfüllen, klicken Sie auf **Nach Abfrage einschließen**.
   - Um eine Regel zu erstellen, die die Gruppe daran hindert, die Objekte aufzunehmen, die bestimmte Suchkriterien erfüllen, klicken Sie auf **Nach Abfrage ausschließen**.
4. Klicken Sie auf der nächsten Seite des Assistenten auf **Hinzufügen**.

   *Wenn Sie den Regeltyp **Nach Abfrage einschließen** oder **Nach Abfrage ausschließen** in Schritt 3 ausgewählt haben, wird das Dialogfeld **Mitgliedschaftsregel erstellen** angezeigt. Andernfalls wird das Dialogfeld **Objekte auswählen** angezeigt.*
5. Schließen Sie das Dialogfeld **Mitgliedschaftsregel erstellen** oder **Objekte auswählen** ab, indem Sie die weiter unten in diesem Abschnitt beschriebenen Verfahren befolgen.
6. Klicken Sie auf **Finish (Fertig stellen)**, um den Assistenten zu schließen.

Gehen Sie folgendermaßen vor, um das Dialogfeld „Mitgliedschaftsregel erstellen" abzuschließen:

1. Wählen Sie in der Liste **Suchen** die Klasse der Objekte aus, die die Mitgliedschaftsregel in die Gruppe aufnehmen oder aus ihr ausschließen soll. Wenn Sie zum Beispiel **Benutzer** auswählen, nimmt die Mitgliedschaftsregel die Benutzer auf bzw. schließt sie aus, die mit den von Ihnen angegebenen Bedingungen übereinstimmen.
2. Wählen Sie in der Liste **In** die Domäne oder den Ordner aus, die bzw. der die Objekte enthält, die die Mitgliedschaftsregel in die Gruppe aufnehmen oder aus ihr ausschließen soll. Wenn Sie zum Beispiel eine Organisationseinheit auswählen, dann nimmt die Mitgliedschaftsregel nur die Objekte auf bzw. schließt sie aus, die in der Organisationseinheit vorhanden sind.

   *Um Ordner zur Liste **In** hinzuzufügen, klicken Sie auf **Durchsuchen** und wählen Sie dann die Ordner im Dialogfeld **Container suchen** aus.*
3. Definieren Sie die Kriterien für die Mitgliedschaftsregel. Um zum Beispiel die Objekte aufzunehmen bzw. auszuschließen, deren Name mit dem Buchstaben „T" beginnen, geben Sie „T" in das Feld **Name** ein. Sie können ein Sternchen (*) als Platzhalter für jede beliebige Zeichenkette verwenden.

4. Klicken Sie optional auf **Regelvorschau**, um eine Liste der Objekte anzuzeigen, die mit den Kriterien übereinstimmen, die Sie definiert haben.
5. Klicken Sie auf **Regel hinzufügen**.

Gehen Sie folgendermaßen vor, um das Dialogfeld „Objekte auswählen" abzuschließen:

1. Klicken Sie in der Liste **Suchen in** auf die Domäne oder den Ordner, der die Objekte enthält, die Sie auswählen möchten. Um einen Ordner zur Liste hinzuzufügen, klicken Sie auf **Durchsuchen**.
2. Führen Sie einen der nachfolgend aufgeführten Schritte durch und klicken Sie dann auf **OK**
   - Doppelklicken Sie in der Liste der Objekte auf das Objekt, das Sie hinzufügen wollen.
   - Geben Sie in das untere Feld den vollständigen Namen oder einen Teil des Namens des Objekts ein, das Sie hinzufügen möchten. Klicken Sie anschließend auf **Namen prüfen**.

- Die einzige Möglichkeit, dynamische Gruppen zu füllen, besteht darin, Mitgliedschaftsregeln hinzuzufügen. Die Mitglieder einer dynamischen Gruppe sind die Objekte, die mit den von den Mitgliedschaftsregeln definierten Kriterien übereinstimmen.
- Klicken Sie zum Zurückkonvertieren einer dynamischen Gruppe in eine Standardgruppe mit der rechten Maustaste auf die Gruppe und klicken Sie dann auf **In Standardgruppe konvertieren**. Beim Konvertieren einer dynamischen Gruppe in eine Standardgruppe entfernt Quest One ActiveRoles alle Mitgliedschaftsregeln aus der Gruppe. Es werden keine Änderungen an der Liste der aktuellen Mitglieder für diese Gruppe vorgenommen.
- Das Dialogfeld **Mitgliedschaftsregel erstellen** ist identisch mit dem Dialogfeld **Suchen**, das Sie für die Suche nach Objekten im Verzeichnis verwenden. Wenn Sie Ihre Suchkriterien angegeben haben, speichert die Funktion **Regel hinzufügen** diese als eine Mitgliedschaftsregel. Weitere Informationen bezüglich der Festlegung von Suchkriterien finden Sie unter Suchen nach Objekten.
- Die Liste **Suchen** umfasst den Eintrag **Benutzerdefinierte Suche**. Durch Auswahl des Eintrags **Benutzerdefinierte Suche** wird die Registerkarte angezeigt, in der Sie mittels erweiterter Optionen benutzerdefinierte Mitgliedschaftsregeln erstellen sowie mittels des LDAP-Protokolls (Lightweight Directory Access Protocol), des Haupt-Zugriffsprotokolls für Active Directory, erweiterte Mitgliedschaftsregeln erstellen können. Weitere Informationen über die Verwendung der erweiterten Suchoptionen finden Sie unter Verfahren zum Verwenden von erweiterten Optionen für die Suche und Verfahren zum Anlegen einer benutzerdefinierten Suche.

Entfernen einer Mitgliedschaftsregel aus einer dynamischen Gruppe

Um eine Mitgliedschaftsregel aus einer dynamischen Gruppe zu entfernen, öffnen Sie das Dialogfeld **Eigenschaften** für die Gruppe. Wählen Sie auf der Registerkarte **Mitgliedschaftsregeln** die zu entfernenden Mitgliedschaftsregeln aus und klicken Sie dann auf **Entfernen**. Klicken Sie danach auf **OK**, um das Dialogfeld **Eigenschaften** zu schließen.

In Quest One ActiveRoles können Mitglieder nicht durch direkte Verwaltung der Mitgliedschaftsliste der Gruppe aus einer dynamischen Gruppe entfernt werden. Um bestimmte Mitglieder zu entfernen, können Sie Regeln der Art **Explizit ausschließen** konfigurieren.

So löschen Sie eine Mitgliedschaftsregel aus einer Gruppe:

1. Wählen Sie in der Konsolenstruktur den Ordner aus, der die Gruppe enthält, aus der Sie eine Mitgliedschaftsregel entfernen möchten.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf die Gruppe und klicken Sie dann auf **Eigenschaften**.

3. Wählen Sie auf der Registerkarte **Mitgliedschaftsregeln** die Mitgliedschaftsregel aus und klicken Sie dann auf **Entfernen**.

Das Dialogfeld Eigenschaften umfasst die Registerkarte Mitgliedschaftsregeln, wenn die ausgewählte Gruppe eine dynamische Gruppe ist. Wenn die Registerkarte Mitgliedschaftsregeln nicht angezeigt wird, dann ist die ausgewählte Gruppe eine Standardgruppe.

Konvertieren einer dynamischen Gruppe in eine Standardgruppe

Beim Konvertieren einer dynamischen Gruppe in eine Standardgruppe werden nur die Mitgliedschaftsregeln aus der Gruppe entfernt. Die Mitgliedschaftsliste der Gruppe bleibt unverändert. Klicken Sie zum Konvertieren einer dynamischen Gruppe in eine Standardgruppe mit der rechten Maustaste auf die Gruppe und klicken Sie dann auf **In Standardgruppe konvertieren**. Klicken Sie im Bestätigungsfeld auf **Ja**.

Wenn eine Gruppe nicht mehr dynamisch ist, wird sie zu einer Standardgruppe mit den folgenden Eigenschaften:

- Im Dialogfeld **Eigenschaften** wird die Registerkarte **Mitgliedschaftsregeln** nicht mehr angezeigt.
- Auf der Registerkarte **Mitglieder** können Sie Mitglieder hinzufügen und entfernen (die Schaltflächen **Hinzufügen** und **Entfernen** werden auf der Registerkarte **Mitglieder** angezeigt).

Ändern, Umbenennen oder Löschen einer dynamischen Gruppe

Sie können dynamische Gruppen auf die gleiche Weise verwalten wie Standardgruppen (reguläre Gruppen): Sie können sie umbenennen, Eigenschaften ändern, ihnen beim Delegieren der Kontrolle einen Trustee zuweisen sowie sie löschen. Die Anweisungen zur Ausführung solcher Verwaltungsaufgaben für dynamische Gruppen sind die gleichen wie bei regulären Gruppen. Schrittweise Anleitungen bezüglich der Verwaltung von Gruppen finden Sie im Abschnitt „Gruppenverwaltungsaufgaben“ im *Quest One ActiveRoles-Benutzerhandbuch* oder in der Quest One ActiveRoles-Hilfe.

Szenario: Automatisches Verschieben von Benutzern zwischen Gruppen

In diesem Szenario wird ein Benutzer aufgrund eines Umzugs von Seattle nach Atlanta aus der Gruppe **Seattle** entfernt und der Gruppe **Atlanta** hinzugefügt.

Angenommen, die Benutzerkonten von Mitarbeitern in Seattle gehören der Gruppe **Seattle** an, und Benutzerkonten von Mitarbeitern in Atlanta gehören der Gruppe **Atlanta** an. Die Gruppe, zu der ein Benutzer gehört, wird durch das Stadtattribut definiert: Bei Mitarbeitern in Seattle hat das Attribut **Stadt** des Benutzerkontos den Wert „Seattle“. Bei Mitarbeitern in Atlanta lautet dieser Wert „Atlanta“.

Führen Sie zum Implementieren dieses Szenarios die folgenden Aktionen aus:

1. Erstellen Sie die Gruppen für Seattle und Atlanta.
2. Konfigurieren Sie Mitgliedschaftsregeln, um Benutzer diesen beiden Gruppen zuzuordnen.Daraufhin gehören nur Benutzerkonten, deren Stadtattributwert „Seattle" lautet, der Gruppe „Seattle" an.

Als Folge zählen nur Benutzerkonten mit dem derzeitigen Ortswert „Seattle" zur Gruppe „Seattle". Wechselt ein Mitarbeiter von Seattle nach Atlanta, ändert ein Administrator das Attribut **Ort** von „Seattle" in „Atlanta", und der Benutzer wird aufgrund der Mitgliedschaftsregel automatisch in die Gruppe **Atlanta** verlagert. Wenn ein Mitarbeiter von Atlanta nach Seattle versetzt wird, ändert ebenfalls ein Administrator das Stadtattribut, und der Benutzer wird automatisch in die Gruppe **Seattle** übertragen.

In den folgenden Abschnitten werden die Schritte zur Implementierung dieses Szenarios detailliert erörtert.

Schritt 1: Erstellen der Gruppen

Um die Gruppe **Seattle** zu erstellen, klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Container, zu dem Sie die Gruppe hinzufügen möchten, und wählen Sie dann **Neu | Gruppe**. Befolgen Sie die Anweisungen des Assistenten unter „Neues Objekt – Gruppe". Geben Sie in das Feld **Gruppenname** den Wert **Seattle** ein.

Um die Gruppe **Atlanta** zu erstellen, klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Container, zu dem Sie die Gruppe hinzufügen möchten, und wählen Sie dann **Neu | Gruppe**. Befolgen Sie die Anweisungen des Assistenten unter „Neues Objekt – Gruppe". Geben Sie in das Feld **Gruppenname** den Wert **Atlanta** ein.

Schritt 2: Konfigurieren der Mitgliedschaftsregeln

In diesem Szenario hat bei Mitarbeitern in Seattle das Attribut **Stadt** des Benutzerkontos den Wert „Seattle". Bei den Mitarbeitern in Atlanta hat es den Wert „Atlanta".

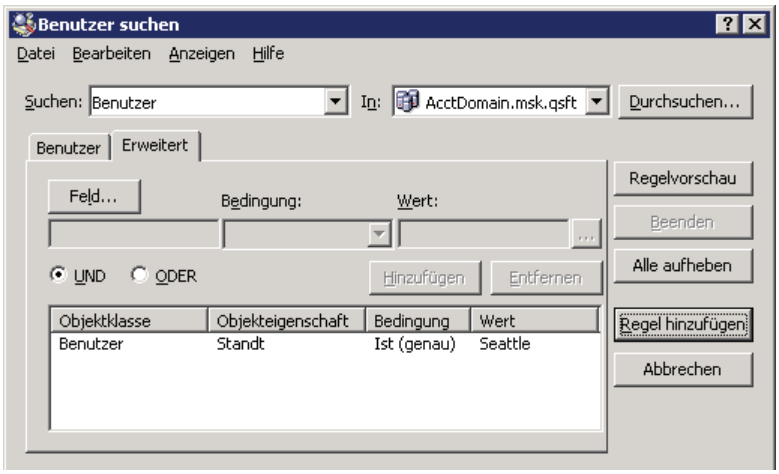
Konfigurieren Sie zuerst die Mitgliedschaftsregel für die Gruppe **Seattle**. Klicken Sie mit der rechten Maustaste auf die Gruppe und klicken Sie dann auf **In dynamische Gruppe konvertieren**. Klicken Sie im Bestätigungsfeld auf **Ja**.

Klicken Sie auf der ersten Seite des Assistenten „Neue Mitgliedschaftsregel" auf **Nach Abfrage einschließen** und klicken Sie dann auf **Weiter**.

Klicken Sie auf der zweiten Seite auf **Hinzufügen**, um das Dialogfeld **Mitgliedschaftsregeln erstellen** anzuzeigen. Konfigurieren Sie dann die Mitgliedschaftsregel anhand der folgenden Schritte:

1. Klicken Sie in der Liste **Suchen** auf **Benutzer**.
2. Klicken Sie auf **Durchsuchen** und wählen Sie die Domäne, Organisationseinheit oder verwaltete Einheit aus, die Benutzerkonten der Mitarbeiter enthält.
3. Klicken Sie auf die Registerkarte **Erweitert**.
4. Klicken Sie auf **Feld**, zeigen Sie auf **Benutzer** und klicken Sie dann auf **Stadt**.
5. Klicken Sie in der Liste **Bedingung** auf **Ist (genau)**.
6. Geben Sie in das Feld **Wert** den Wert **Seattle** ein.
7. Klicken Sie auf **Hinzufügen**.

Nach der Ausführung dieser Schritte entspricht das Dialogfeld der folgenden Abbildung.



Klicken Sie auf die Schaltfläche **Regel hinzufügen**. Klicken Sie dann im Assistenten „Neue Mitgliedschaftsregel" auf **Fertig stellen**, um den Vorgang abzuschließen.

Jetzt ist die Gruppe **Seattle** so konfiguriert, dass sie die Benutzerkonten einschließt, deren Attribut **Stadt** den Wert „Seattle" aufweist.

Wiederholen Sie den gleichen Vorgang für die Gruppe **Atlanta**, aber geben Sie beim Konfigurieren der Mitgliedschaftsregel in das Feld **Wert** den Wert **Atlanta** ein.

10

Berichte in Quest One ActiveRoles

- Einleitung
- Datenvorbereitungs-Collector für Berichte
- Quest Knowledge Portal für die Anzeige von Berichten
- Arbeiten mit Berichten

Einleitung

Die Quest One ActiveRoles-Berichterstattungslösung macht Microsoft SQL Server Reporting Services (SSRS) zu einer Plattform für die Verwaltung, Erzeugung und Anzeige von Berichten.

Durch die Nutzung von SSRS bietet Quest One ActiveRoles Berichterstattungsfunktionen der Unternehmensklasse, die die Vorteile von webbasierten Funktionen mit der herkömmlichen Berichterstattung kombinieren. Die Verwendung von Reporting Services bietet die Möglichkeit zur Zentralisierung der Berichtsspeicherung und -verwaltung, einen sicheren Zugriff auf Berichte, die Kontrolle über die Verarbeitung und Verbreitung der Berichte sowie Standards bezüglich der Verwendung der Berichte.

Eine umfassende Sammlung von Berichtsdefinitionen, die als das *Quest One ActiveRolesReport Pack* bezeichnet werden, werden auf dem Berichtsserver, einer Komponente von Reporting Services, veröffentlicht. Durch die Installation von Report Pack werden veröffentlichte Berichte erstellt, auf die über Webadressen (URLs), über SharePoint Web-Komponenten oder über Report Manager, ein im Lieferumfang von SSRS enthaltenes, webbasiertes Berichtszugriffs- und Verwaltungstool, zugegriffen werden kann.

Eine weitere Option für den Zugriff auf veröffentlichte Berichte ist das Quest Knowledge Portal, eine webbasierte Anwendung, die die Funktionen von SSRS erweitern, um eine einfache Berichtsverwaltung und -bereitstellung zu ermöglichen. Mit Quest Knowledge Portal kann ein Administrator schnell und einfach Berichte in einer Ordnerhierarchie organisieren, Datenquellen konfigurieren, Berichtseigenschaften ändern, Berichte exportieren und importieren und die Berichte durchsuchen.

Durch Öffnen eines veröffentlichten Berichts vom Berichtsserver wird der Bericht in einem für die Anzeige geeigneten Format generiert. Diese Aktion wird *Generierung eines Berichts* genannt. Die Generierung eines Berichts erfolgt auch bei einem Abonnement, wenn der Bericht an ein E-Mail-Eingangsfach oder an eine Dateifreigabe in einem vom Berichtsbenutzer angegebenen Ausgabeformat gesendet wird.

Standardmäßig generiert der Berichtsserver die Berichte im HTML-Format. Zusätzlich zu HTML können die Berichte in einer Vielzahl von Ausgabeformaten einschließlich Excel, XML, PDF, TIFF und CSV generiert werden. Berichtsbenutzer können wählen, ob die Berichte auf Anforderung in einem bevorzugten Format für die Datenbearbeitung generiert oder ausgedruckt werden.

Die Berichte, die generiert werden können, sobald Quest One ActiveRoles Report Pack installiert ist, sind ganz entscheidend für Überprüfung und Verfolgung von Änderungen, für die Überwachung und Analyse von Verzeichnisdaten und für die Bewertung der Quest One ActiveRoles Server Sicherheits- und Richtlinienkonfigurationen. Die Berichte lassen sich in die folgenden Kategorien einteilen:

- **Quest One ActiveRoles-Verlaufsprotokoll.** Überprüfen Sie, welche Änderungen mit Hilfe von ActiveRoles an den Verzeichnisdaten vorgenommen wurden, wer diese Änderungen vorgenommen hat und wann diese Änderungen erfolgt sind.
- **Active Directory-Bewertung.** Untersuchen Sie den Status von Verzeichnisdaten wie etwa die Eigenschaften von Benutzern, Gruppen und anderen Verzeichnisobjekten, Gruppenmitgliedschaftslisten und die Inhalte von Organisationseinheiten.
- **Administratorfunktionen.** Zeigen Sie Details darüber an, wer bei Verwendung von Quest One ActiveRoles Zugriff auf welche Daten hat und welche Änderungen administrative Benutzer oder Gruppen vornehmen dürfen.
- **Verwaltete Einheiten.** Zeigen Sie Details zu den in der Quest One ActiveRoles-Umgebung definierten verwalteten Einheiten an, welche Richtlinien auf die verwalteten Einheiten angewandt sind und welche Benutzer oder Gruppen über einen administrativen Zugriff auf welche verwalteten Einheiten verfügen.

- **Richtlinienobjekte.** Zeigen Sie Details dazu an, welche administrative Richtlinien in der Quest One ActiveRoles-Umgebung definiert sind, wo bestimmte Richtlinien angewandt werden und welche Richtlinien für bestimmte Objekte und Container in Kraft sind.
- **Richtlinienkonformität.** Zeigen Sie Details dazu an, welche Daten im Verzeichnis nicht mit den gültigen Quest One ActiveRoles-Richtlinien konform sind und gegen welche Richtlinienregeln verstoßen wurde.

Berichte werden auf der Grundlage der vom Quest One ActiveRoles Collector vorbereiteten Daten erstellt. Nähere Informationen zum Quest One ActiveRoles Collector finden Sie unter „Collector für die Vorbereitung der Berichtsdaten" weiter unten in diesem Kapitel.

Sie können Berichte mit Hilfe von Report Manager, einem Bestandteil von SSRS, generieren und anzeigen. Eine weitere Möglichkeit, Berichte zu generieren und anzuzeigen, ist die Nutzung von Quest Knowledge Portal, einem webbasierten Berichtsmanagementtool von Quest Software. Quest Knowledge Portal bietet eine einfache und bequeme Möglichkeit der Generierung und Anzeige von Berichten, die auf vom Quest One ActiveRoles Collector erfassten Daten beruhen. Nähere Informationen über das Quest Knowledge Portal finden Sie unter „Quest Knowledge Portal für die Anzeige von Berichten" weiter unten in diesem Kapitel. Weitere Informationen über das Quest Knowledge Portal finden Sie in der diesem Produkt beiliegenden Dokumentation.

Anweisungen bezüglich der Generierung und Anzeige von Berichten finden Sie unter „Arbeiten mit Berichten" weiter unten in diesem Kapitel.

Datenvorbereitungs-Collector für Berichte

Mit dem Collector von Quest One ActiveRoles können Sie Daten von Computern sammeln, auf denen der Verwaltungsdienst ausgeführt wird, und diese Daten in einer SQL Server-Datenbank speichern, sodass die Daten für die Berichterstattung verfügbar werden.

Der Quest One ActiveRoles Collector wird als eine separate Komponente von Quest One ActiveRoles installiert.

Daten für Berichte werden aus den folgenden Quellen gesammelt:

- **Active Directory.** Der Collector greift über den Verwaltungsdienst auf Active Directory zu. Berichte, die auf diesen Daten basieren, enthalten detaillierte Informationen zu Domänen, Konten, Gruppen und anderen Active Directory-Objekten.
- **Quest One ActiveRoles-Konfigurationsdatenbank.** Berichte, die auf diesen Daten basieren, enthalten detaillierte Informationen dazu, wer mit Quest One ActiveRoles welche Aktionen für welche Verzeichnisobjekte ausführen kann. Außerdem enthalten sie Informationen zu den von Quest One ActiveRoles definierten Richtlinien.
- **Ereignisprotokoll auf Computern, auf denen der Verwaltungsdienst ausgeführt wird.** Berichte, die auf diesen Daten basieren, enthalten detaillierte Informationen zu ausgeführten Aktionen, zum Erfolg oder Misserfolg jeder Aktion sowie zu Objekteigenschaften, die mit Quest One ActiveRoles geändert wurden.

Der Bereich der Daten, die der Collector aus Active Directory abrufen kann, wird durch die Zugriffsrechte des Benutzerkontos beschränkt, mit dem der Collector die Datenerfassungsaufgabe ausführt. Daher können Berichte, die auf Active Directory-Daten basieren, nur Informationen zu den Objekten enthalten, auf die der Collector in Active Directory zugreifen darf.

Nehmen Sie beispielsweise an, dass der Collector eine Datenerfassungsaufgabe mit dem Benutzerkonto ausführt, das nicht über Zugriffsrechte für Benutzerkontoeigenschaften in Active Directory verfügt. Dann kann der Collector keine Daten zu Benutzerkonten abrufen, und in den Berichten sind keine Informationen zu Benutzerkonten enthalten, auch nicht die Anzahl der Benutzerkonten.

Um Daten für Berichte zu sammeln, starten Sie den Assistenten für den Quest One ActiveRoles Collector: Klicken Sie auf **Start** und wählen Sie dann **Alle Programme | Quest Software | Quest One ActiveRoles | Collector**. Klicken Sie dann im Assistenten auf **Weiter**, um die Seite **Aufgabe auswählen** anzuzeigen.

Auf der Seite **Aufgabe auswählen** können Sie eine der folgenden Aufgaben für die Ausführung auswählen:

- **Collect data from the network (Daten aus dem Netzwerk erfassen).** Sammelt Daten und Ereignisse von den Computern, auf denen der Verwaltungsdienst ausgeführt wird, und speichert die gesammelten Information in einer SQL Server-Datenbank, um die Informationen für den Berichtsserver verfügbar zu machen.
- **Process gathered events (Vom Prozess erfasste Ereignisse).** Exportiert ausgewählte Ereignisse in eine andere SQL Server-Datenbank oder löscht veraltete Informationen aus der Datenbank.

Sammeln von Daten aus dem Netzwerk

Wenn Sie auf der Seite **Select Task (Aufgabe auswählen)** die Option **Collect data from the network (Daten aus dem Netzwerk erfassen)** auswählen, zeigt der Assistent im nächsten Schritt die Seite **Configure Connection (Verbindung konfigurieren)** an.

Auf der Seite **Configure Connection** (Verbindung konfigurieren) des Assistenten werden Sie aufgefordert, die anfänglichen Optionen für die Verwaltung der Daten anzugeben: Datenbank, in der die erfassten Daten gespeichert werden sollen; Quellcomputer, auf dem der Verwaltungsdienst ausgeführt wird; geben Sie auch die Anmeldeinformationen für die Anmeldung bei diesem Computer an.

Um eine Datenbank anzugeben oder eine andere Datenbank auszuwählen, klicken Sie auf **Browse (Durchsuchen)**. Damit können Sie auf den Assistenten „SQL Server-Verbindung" zugreifen, der Sie durch den Konfigurationsvorgang für die Verbindung mit der Datenbank führt.

Geben Sie im Feld **ActiveRoles-Dienst** den vollständigen Namen des Computers mit dem Verwaltungsdienst an, von dem Sie Informationen sammeln möchten.

Geben Sie im Bereich **Log on as (Anmelden als)** die Rechtezuweisungen an, mit denen der Collector sich beim Verwaltungsdienst anmelden soll. Sie können eine der folgenden Optionen auswählen:

- **Current user (Aktueller Benutzer).** Stellt die Verbindung zum Verwaltungsdienst mit den Rechtezuweisungen des Benutzerkontos her, mit dem der Collector gestartet wird.
- **Specified user (Angegebener Benutzer).** Stellt die Verbindung zum Verwaltungsdienst mit den angegebenen Rechtezuweisungen her (Benutzername und Kennwort).

Klicken Sie auf **Next (Weiter)**, um mit der Seite **Data Collection Tasks (Datenerfassungsaufgaben)** fortzufahren.

Auf der Seite **Data Collection Tasks (Datenerfassungsaufgaben)** des Assistenten werden Sie aufgefordert, die Quellen der zu sammelnden Daten anzugeben. Sie können folgende Quellen auswählen:

- **Active Directory.** Informationen zu Benutzern, Gruppen, Computern, Organisationseinheiten und Domänen von Active Directory.
- **Richtlinienkonformitätsinformationen.** Informationen darüber, ob die Active Directory-Daten mit den von Quest One ActiveRoles definierten Richtlinien konform sind oder nicht. Erfordert, dass Daten auch von Active Directory erfasst werden (das Kontrollkästchen **Active Directory** muss aktiviert sein).
- **EDM Server Event Log (EDM Server-Ereignisprotokoll).** Informationen aus dem **EDM-Server**-Ereignisprotokoll auf dem Computer, auf dem der Verwaltungsdienst ausgeführt wird.

Klicken Sie auf **Next (Weiter)** um mit der Seite **Data to Collect (Zu erfassende Daten)** fortzufahren.

Der Assistent zeigt die Seite **Data to Collect (Zu erfassende Daten)** nur an, wenn Sie auf der Seite **Data Collection Tasks (Datenerfassungsaufgaben)** das Kontrollkästchen **Active Directory** aktivieren.

Auf der Seite **Data to Collect (Zu erfassende Daten)** des Assistenten werden Sie aufgefordert, die Kategorien der zu sammelnden Daten anzugeben. Sie können folgende Kategorien auswählen:

- **Zugriffsvorlagen.** Informationen zu Zugriffsvorlagen, die in der Quest One ActiveRoles-Umgebung definiert sind.
- **Richtlinienobjekte.** Informationen zu Richtlinienobjekten, die in der Quest One ActiveRoles-Umgebung definiert sind.
- **Verwaltete Einheiten.** Informationen zu verwalteten Einheiten, die in der Quest One ActiveRoles-Umgebung definiert sind.
- **Group Policy (Gruppenrichtlinie).** Gruppenrichtlinienbezogene Informationen.
- **Skriptmodule.** Informationen zu Skriptmodulen, die in der Quest One ActiveRoles-Umgebung definiert sind.

Wenn Sie auf der vorigen Seite das Kontrollkästchen **Policy Compliance Information (Richtlinienkonformitätsinformationen)** aktiviert haben, können Sie auf der Seite **Data to Collect (Zu erfassende Daten)** das Kontrollkästchen **Policy Objects (Richtlinienobjekte)** nicht deaktivieren.

Klicken Sie auf **Next (Weiter)**, um mit der Seite **Select Domains or OUs (Domänen oder Organisationseinheiten auswählen)** fortzufahren.

Auf der Seite **Select Domains or OUs (Domänen oder Organisationseinheiten auswählen)** des Assistenten werden Sie aufgefordert, die Domänen oder Container anzugeben, aus denen Sie Informationen sammeln möchten. Sie können diese Seite wie folgt ausfüllen:

- Klicken Sie auf **Add (Hinzufügen)**, um der Liste auf der Seite eine Domäne oder Organisationseinheit hinzuzufügen.
- Klicken Sie auf **Remove (Entfernen)**, um eine ausgewählte Domäne oder Organisationseinheit aus der Liste zu löschen.

Wenn Sie eine Domäne oder Organisationseinheit auswählen, können Sie wie folgt erzwingen, dass der Assistent Informationen über alle untergeordneten Objekte der ausgewählten Domäne oder Organisationseinheit erfassen soll: Aktivieren Sie in dem Dialogfeld, das durch Klicken auf **Add (Hinzufügen)** angezeigt wird, das Kontrollkästchen **Use subtree search (Teilstruktursuche verwenden)**. Wenn Sie das Kontrollkästchen **Use subtree search (Teilstruktursuche verwenden)** deaktivieren, erfasst der Assistent nur Informationen über die unmittelbaren untergeordneten Objekte der ausgewählten Domäne oder Organisationseinheit.

Klicken Sie auf **Next (Weiter)**, um mit der Seite **Select Operation Mode (Betriebsart auswählen)** fortzufahren.

Auf der Seite **Select Operation Mode (Vorgangsmodus auswählen)**können Sie angeben, dass die Taskausführung sofort gestartet werden soll, oder Sie können sie für einen passenden Zeitpunkt planen. Sie können auch die SID-Auflösung deaktivieren, damit Daten schneller gesammelt werden.

Wenn Sie den Sammlungsprozess sofort starten möchten, wählen Sie unter **Quest One ActiveRoles Collector ausführen** die Option **Jetzt** aus und klicken Sie auf **Weiter**. Während der Assistent den Vorgang ausführt, wird der Statusbildschirm angezeigt, in dem der Fortschritt detailliert zu erkennen ist.

Nach Abschluss des Vorgangs wird das Abschlussfenster des Assistenten mit den Vorgangsergebnissen angezeigt. Sie können auf **View Log (Protokoll anzeigen)** klicken, um das Vorgangsprotokoll auf etwaige Fehler zu untersuchen.

Wenn Sie für den Task einen Zeitplan festlegen möchten, wählen Sie **On schedule (Nach Zeitplan)** aus und klicken Sie auf **Next (Weiter).** Dann wird die Seite **Schedule (Zeitplan)** angezeigt, auf der Sie den Zeitplan und das Anmeldekonto für den Task angeben können. Klicken Sie auf **Change (Ändern)**, um einen Zeitplan für den Task zu erstellen. Klicken Sie auf **Account (Konto)**, um den Benutzernamen und das Kennwort des Benutzerkontos anzugeben, mit dem der Task ausgeführt werden soll. Wenn Sie die Zeitplanoptionen festgelegt haben, klicken Sie auf **Next (Weiter)**, um den Assistenten abzuschließen.

Verfahren zum Sammeln von Daten aus dem Netzwerk

Der Quest One ActiveRoles Collector wird für die Vorbereitung von Daten zu Berichtszwecken verwendet. Die Daten werden in der von Ihnen angegebenen Datenbank gespeichert. Um die Daten dann für den Berichtsserver verfügbar zu machen, müssen Sie die Datenquelle auf dem Berichtsserver so konfigurieren, dass sie eine Verbindung zu der Datenbank herstellt, in der sich die Daten befinden. Dieses Thema enthält Anweisungen bezüglich der Vorbereitung von Berichtsdaten. Anweisungen bezüglich der Konfiguration der Datenquelle für Quest One ActiveRoles Report Pack finden Sie unter Konfigurieren der Datenquelle weiter unten in diesem Kapitel.

Gehen Sie folgendermaßen vor, um Daten aus dem Netzwerk zu erfassen:

1. Um den Quest One ActiveRoles Collector-Assistenten zu starten, klicken Sie auf **Start** und wählen Sie **Alle Programme | Quest Software | Quest One ActiveRoles| Collector**.
2. Folgen Sie den Anweisungen des Assistenten.
3. Aktivieren Sie auf der Seite **Select Task (Aufgabe auswählen)** die Option **Collect data from the network (Daten aus dem Netzwerk erfassen)**.

4. Geben Sie auf der Seite **Configure Connection (Verbindung konfigurieren)** die Datenbank an, in der die erfassten Daten gespeichert werden sollen; Quellcomputer, auf dem der Verwaltungsdienst ausgeführt wird; geben Sie auch die Anmeldeinformationen für die Anmeldung bei diesem Computer an.
   a) Um erstmals eine Datenbank anzugeben oder eine andere Datenbank auszuwählen, klicken Sie auf **Browse (Durchsuchen)**und verwenden Sie dann den SQL Server-Verbindungsassistenten, um die Verbindung zur Datenbank zu konfigurieren.
   b) Geben Sie im Feld **ActiveRoles-Dienst** den vollständigen Namen des Computers an, auf dem der Verwaltungsdienst ausgeführt wird, von dem Sie die Informationen erfassen möchten.
   c) Klicken Sie unter **Log on as (Anmelden als)** auf eine der folgenden Optionen:
      - **Current user (Aktueller Benutzer)**, um eine Verbindung zu dem Verwaltungsdienst mit dem Benutzerkonto herzustellen, mit dem der Collector gestartet wird.
      - **Specified user (Angegebener Benutzer)**, um den Benutzernamen und das Kennwort anzugeben, den bzw. das der Collector für den Verbindungsaufbau zum Verwaltungsdienst verwenden soll.
5. Geben Sie auf der Seite **Data Collection Tasks (Datenerfassungsaufgaben)** die Quellen der zu erfassenden Daten an. Aktivieren oder deaktivieren Sie diese Kontrollkästchen:
   - **Active Directory**, um Informationen zu Benutzern, Gruppen, Computern, Organisationseinheiten und Domänen von Active Directory zu erfassen.
   - **Richtlinienkonformitätsinformationen** zur Erfassung von Informationen darüber, ob die Active Directory-Daten mit den von Quest One ActiveRoles definierten Richtlinien konform sind oder nicht; wenn Sie dieses Kontrollkästchen aktivieren, stellen Sie sicher, dass auch das Kontrollkästchen **Active Directory** aktiviert ist.
   - **EDM Server Event Log (EDM Server-Ereignisprotokoll)**, um Informationen aus dem „EDM Server"-Ereignisprotokoll auf dem Computer, auf dem der Verwaltungsdienst ausgeführt wird, zu erfassen.
6. Geben Sie auf der Seite **Zu erfassende Daten** die Kategorien der im Zusammenhang mit Quest One ActiveRoles stehenden Daten an, aus denen Sie die Daten erfassen möchten. Aktivieren oder deaktivieren Sie diese Kontrollkästchen:
   - **Zugriffsvorlagen** zur Sammlung von Informationen zu Zugriffsvorlagen, die in der Quest One ActiveRoles-Umgebung definiert sind.
   - **Richtlinienobjekte** zur Sammlung von Informationen zu Richtlinienobjekten in der Quest One ActiveRoles-Umgebung.
   - **Verwaltete Einheiten** zur Sammlung von Informationen zu verwalteten Einheiten, die in der Quest One ActiveRoles-Umgebung definiert sind.
   - **Group Policy (Gruppenrichtlinie)**, um in Zusammenhang mit der Gruppenrichtlinie stehende Informationen zu erfassen.
   - **Skriptmodule** zur Sammlung von Informationen zu Skriptmodulen, die in der Quest One ActiveRoles-Umgebung definiert sind.
7. Geben Sie auf der Seite **Select Domains or OUs (Domänen oder Organisationseinheiten auswählen)**die Domänen oder Container an, aus denen Sie Informationen sammeln möchten.
   - Klicken Sie auf **Add (Hinzufügen)**, um der Liste auf der Seite eine Domäne oder Organisationseinheit hinzuzufügen.
   - Klicken Sie auf **Remove (Entfernen)**, um eine ausgewählte Domäne oder Organisationseinheit aus der Liste zu löschen.

*Wenn Sie eine Domäne oder Organisationseinheit auswählen, können Sie wie folgt erzwingen, dass der Assistent Informationen über alle untergeordneten Objekte der ausgewählten Domäne oder Organisationseinheit erfassen soll: Aktivieren Sie in dem Dialogfeld, das durch Klicken auf **Add (Hinzufügen)** angezeigt wird, das Kontrollkästchen **Use subtree search (Teilstruktursuche verwenden)**. Wenn Sie das Kontrollkästchen **Use subtree search (Teilstruktursuche verwenden)** deaktivieren, erfasst der Assistent nur Informationen über die unmittelbaren untergeordneten Objekte der ausgewählten Domäne oder Organisationseinheit.*

8. Geben Sie auf Seite **Select Operation Mode (Vorgangsmodus auswählen)** an, ob die Aufgabenausführung sofort gestartet werden soll oder ob die Aufgabenausführung für einen passenden Zeitpunkt geplant werden soll:
   - Um den Erfassungsvorgang direkt zu starten, klicken Sie auf **Now (Jetzt)** und klicken Sie dann auf **Next (Weiter)**.
   - Um die Aufgabe zu planen, wählen Sie **On schedule (Nach Zeitplan)** aus und klicken Sie dann auf **Next (Weiter)**.
9. Wenn Sie die Option **On schedule (Nach Zeitplan)** ausgewählt haben, dann geben Sie auf der Seite **Schedule (Zeitplan)** den Aufgabenzeitplan und das Anmeldekonto an:
   - Klicken Sie auf **Change (Ändern)**, um einen Zeitplan für den Task zu erstellen.
   - Klicken Sie auf **Account (Konto)**, um den Benutzernamen und das Kennwort des Benutzerkontos anzugeben, mit dem der Task ausgeführt werden soll.

Verarbeiten gesammelter Ereignisse

Wenn Sie die Option **Process gathered events (Gesammelte Ereignisse verarbeiten)** auf der Seite **Select Task (Aufgabe auswählen)** auswählen, zeigt der Assistent im nächsten Schritt die Seite **Data Processing Task (Datenverarbeitungsaufgabe)** an.

Auf der Seite **Data Processing Task (Datenverarbeitungsaufgabe)** des Assistenten geben Sie an, was mit den Ereignissen geschehen soll, die von Verwaltungsdienstcomputern gesammelt und in der Datenbank gespeichert wurden. Sie können eine der folgenden Optionen auswählen:

- **Export using date range (Exportieren mit Hilfe des Datumsbereichs).** Geben Sie den Datumsbereich für die Ereignisse an, die Sie exportieren möchten. Die Zeitpunkte, die Sie angeben, werden als Greenwich Mean Time (GMT) interpretiert.
- **Export events older than (Exportieren von Ereignissen, die älter sind als).** Geben Sie den Altersgrenzwert für die Ereignisse an, die Sie exportieren möchten.
- **Delete events older than (Löschen von Ereignissen, die älter sind als).** Geben Sie den Altersgrenzwert für die Ereignisse an, die Sie löschen möchten.

Klicken Sie auf **Next (Weiter)**, um die Seite **Source Database (Quelldatenbank)** anzuzeigen. Auf dieser Seite können Sie die Datenbank auswählen, aus der Sie Informationen exportieren oder löschen möchten. Außerdem können Sie hier die Anmeldeeinstellung für die Verbindung mit SQLServer festlegen. Um eine Datenbank auszuwählen, klicken Sie auf **Browse (Durchsuchen)**. Damit können Sie auf den Assistenten „SQL Server-Verbindung" zugreifen, der Sie durch den Konfigurationsvorgang für die Verbindung mit der Datenbank führt.

Klicken Sie auf **Next (Weiter)**, um den Vorgang fortzusetzen.

Wenn Sie die Exportoption für Informationen ausgewählt haben, zeigt der Assistent die Seite **Target Database (Zieldatenbank)** an. Diese ähnelt der Seite **Source Database (Quelldatenbank)**. Auf der Seite **Zieldatenbank** können Sie die Datenbank auswählen, in die Sie Informationen exportieren möchten. Außerdem können Sie hier die Anmeldeeinstellung für die Verbindung mit SQL Server

festlegen. Um eine Datenbank auszuwählen, klicken Sie auf **Browse (Durchsuchen)**. Damit können Sie auf den Assistenten „SQL Server-Verbindung" zugreifen, der Sie durch den Konfigurationsvorgang für die Verbindung mit der Datenbank führt. Klicken Sie danach auf **Next (Weiter)**, um den Vorgang zu starten.

Während der Assistent den ausgewählten Vorgang ausführt, wird der Statusbildschirm angezeigt, in dem der Fortschritt detailliert zu erkennen ist. Nach Abschluss des Vorgangs wird das Abschlussfenster des Assistenten mit den Vorgangsergebnissen angezeigt. Sie können auf **View Log (Protokoll anzeigen)** klicken, um das Vorgangsprotokoll auf etwaige Fehler zu untersuchen.

Verfahren zur Verarbeitung von erfassten Ereignissen

Gehen Sie folgendermaßen vor, um erfasste Ereignisse zu verarbeiten:

1. Um den Quest One ActiveRoles Collector-Assistenten zu starten, klicken Sie auf **Start** und wählen Sie **Alle Programme | Quest Software | Quest One ActiveRoles| Collector**.
2. Folgen Sie den Anweisungen des Assistenten.
3. Aktivieren Sie auf der Seite **Select Task (Aufgabe auswählen)** die Option **Process gathered events (Gesammelte Ereignisse verarbeiten)**.
4. Geben Sie auf der Seite **Data Processing Task (Datenverarbeitungsaufgabe)** an, was mit den Ereignissen geschehen soll, die von Verwaltungsdienstcomputern gesammelt und in der Datenbank gespeichert wurden. Wählen Sie eine der folgenden Optionen aus:
   - **Export using date range (Exportieren mit Hilfe des Datumsbereichs).** Geben Sie den Datumsbereich für die Ereignisse an, die Sie exportieren möchten. Die Zeitpunkte, die Sie angeben, werden als Greenwich Mean Time (GMT) interpretiert.
   - **Export events older than (Exportieren von Ereignissen, die älter sind als).** Geben Sie den Altersgrenzwert für die Ereignisse an, die Sie exportieren möchten.
   - **Delete events older than (Löschen von Ereignissen, die älter sind als).** Geben Sie den Altersgrenzwert für die Ereignisse an, die Sie löschen möchten.
5. Klicken Sie auf der Seite **Source Database (Quelldatenbank)** auf **Browse (Durchsuchen)** und verwenden Sie dann den SQL Server-Verbindungsassistenten, um die Verbindung zu der Datenbank zu konfigurieren, aus der Sie die Ereignisse exportieren oder löschen möchten.
6. Klicken Sie auf der Seite **Target Database (Zieldatenbank)** auf **Browse (Durchsuchen)** und verwenden Sie dann den SQL Server-Verbindungsassistenten, um die Verbindung zu der Datenbank zu konfigurieren, in die Sie die Ereignisse importieren möchten.

Quest Knowledge Portal für die Anzeige von Berichten

Quest Knowledge Portal ist ein webbasiertes Berichterstattungstool, das Microsoft SQL Server Reporting Services (SSRS) um zusätzliche Optionen erweitert, um eine einfache Berichtsverwaltung und -bereitstellung zu ermöglichen. Mit Quest Knowledge Portal können Sie folgende Aktionen ausführen:

- Anzeigen von Berichten über vom Quest One ActiveRoles Collector vorbereitete Daten
- Abonnieren der Berichte
- Durchsuchen der Berichte nach den von Ihnen benötigten Informationen
- Starten von Report Builder zur Erstellung von benutzerdefinierten Berichten
- Erstellen einer hierarchischen Struktur für die Berichtsordner
- Anzeigen oder Ändern der Eigenschaftseinstellungen für Berichte und Ordner

Anweisungen bezüglich der Installation und der Verwendung dieses Tools finden Sie in der im Lieferumfang von Quest Knowledge Portal enthaltenen Dokumentation. Dieser Abschnitt enthält eine kurze Übersicht über einige grundlegende Optionen von Quest Knowledge Portal.

Verwalten von Berichten und Ordnern

Um Berichte und Berichtsordner in Quest Knowledge Portal zu verwalten, klicken Sie auf die Registerkarte **Berichte** im linken Bereich des Quest Knowledge Portal-Fensters.

Klicken Sie anschließend durch die Berichtsordner, um den gewünschten Bericht zu suchen, und klicken Sie dann auf den Namen des Berichts. Sie können die folgenden Optionen auswählen:

- **Bericht anzeigen.** Öffnen Sie die Berichtsanzeigeseite, auf der Sie Berichtsparameter festlegen und den Bericht generieren und anzeigen können.
- **Bericht in einem neuen Fenster anzeigen.** Öffnen Sie die Berichtsanzeigeseite in einem separaten Fenster.
- **Sicherheitseinstellungen.** Kontrollieren Sie den Benutzerzugriff auf den Bericht, indem Sie Benutzern oder Gruppen die entsprechenden Rollen in SSRS zuweisen.
- **Berichtseigenschaften.** Zeigen Sie die Eigenschaften des Berichts an oder ändern Sie diese.
- **Berichtsansicht anpassen.** Ändern Sie die Art und Weise, wie Daten angezeigt werden, wenn der Bericht generiert wird.
- **Bericht entfernen.** Löschen Sie die Berichtsdefinition vom Berichtsserver.

Wenn Sie einen Berichtsordner auswählen, sind die folgenden Optionen verfügbar:

- **Neuer Ordner.** Erstellen Sie einen neuen Ordner innerhalb des von Ihnen ausgewählten Ordners.
- **Ordnereigenschaften.** Zeigen Sie die Eigenschaften des Ordners an oder ändern Sie diese.
- **Sicherheitseinstellungen.** Kontrollieren Sie den Benutzerzugriff auf den Ordner, indem Sie Benutzern oder Gruppen die entsprechenden Rollen in SSRS zuweisen.
- **Berichte organisieren.** Passen Sie die Struktur der Ordner an und ordnen Sie die Berichte nach Ordnern an.
- **Ordner löschen.** Löschen Sie den Ordner sowie dessen gesamten Inhalt.

Sie können Berichte nach deren Namen suchen. Klicken Sie auf die Registerkarte „Suchen" im linken Bereich des Quest Knowledge Portal-Fensters, um eine Seite anzuzeigen, auf der Sie einen Namen eingeben können, und starten Sie dann Ihre Suche.

Weitere Informationen und Anweisungen finden Sie in der Hilfe von Quest Knowledge Portal. Um während der Verwendung von Quest Knowledge Portal Hilfethemen anzuzeigen, klicken Sie auf die Verknüpfung **Hilfe**.

Arbeiten mit Berichten

Der Quest One ActiveRoles Collector wird für die Vorbereitung von Daten zu Berichtszwecken verwendet. Die Daten werden in der Datenbank gespeichert, die Sie bei der Konfiguration des Datenerfassungsauftrags angeben (siehe „Collector zur Vorbereitung von Daten für Berichte" weiter oben in diesem Kapitel). Um die Daten für den Berichtsserver verfügbar zu machen, muss die Datenquelle auf dem Berichtsserver so konfiguriert werden, dass sie eine Verbindung zu der Datenbank herstellt, in der sich die Berichtsdaten befinden. Dann können Sie Quest One ActiveRoles-Berichte generieren und anzeigen.

Konfigurieren der Datenquelle

Normalerweise wird die Datenquelle während der Installation von Report Pack konfiguriert. Wenn die Datenquelle nicht auf diese Weise konfiguriert wurde oder die Konfiguration der Datenquelle geändert werden muss, dann befolgen Sie die nachfolgend aufgeführten Anweisungen. Die Anweisungen setzen voraus, dass Quest One ActiveRoles Report Pack auf dem Berichtsserver installiert ist, den Sie konfigurieren möchten.

Gehen Sie folgendermaßen vor, um die Datenquelle mit Hilfe von SSRS Report Manager zu konfigurieren:

1. Starten Sie SSRS Report Manager und rufen Sie die Seite **Inhalt** auf.

   Report Manager wird während der Einrichtung von SQL Server Reporting Services (SSRS) auf demselben Computer wie der Berichtsserver installiert. Um Report Manager zu starten, öffnen Sie Microsoft Internet Explorer 6.0 oder höher. Geben Sie in das Adressfeld von Internet Explorer den Report Manager URL ein. Standardmäßig lautet der URL http://<Computername>/reports.

2. Gehen Sie auf der Seite **Inhalt** folgendermaßen vor:
   a) Klicken Sie auf **QKP**.
   b) Klicken Sie auf **SharedDataSources**.
   c) Klicken Sie auf die Datenquelle mit dem Namen **Quest One ActiveRoles6.8.0-Berichtsdaten**.

   *Wenn das Element **SharedDataSources** nicht auf der Seite **Inhalt** angezeigt wird, klicken Sie auf **Details anzeigen** oder **Detailansicht** (in Abhängigkeit von Ihrer SSRS-Version).*

3. Geben Sie auf der Seite **Eigenschaften** im Feld **Verbindungszeichenkette** die SQL Server-Instanz und den Namen der Datenbank, in der sich die von Quest One ActiveRoles Collector vorbereiteten Berichtsdaten befinden, an.

   Wenn der Name der Datenbank zum Beispiel „ARServerReporting" lautet und sich die Datenbank auf der SQL Server-Instanz mit dem Namen „MyServer\Enterprise" befindet, dann lautet die Verbindungszeichenkette wie folgt:

   ```
   data source = MyServer\Enterprise ; initial catalog = ARServerReporting
   ```

4. Klicken Sie auf **Anwenden**.

Wenn Quest Knowledge Portal installiert ist, können Sie die Datenquelle mit Hilfe von Quest Knowledge Portal konfigurieren.

Gehen Sie folgendermaßen vor, um die Datenquelle mit Hilfe von Quest Knowledge Portal zu konfigurieren:

1. Öffnen Sie die Knowledge Portal-Startseite.

   Um die Knowledge Portal-Startseite zu öffnen, geben Sie den Knowledge Portal-URL in das Adressfeld von Internet Explorer ein. Standardmäßig lautet der URL http://<Computername>/QKP.

2. Klicken Sie im linken Bereich des Knowledge Portal-Fensters auf **Datenquellen** und wählen Sie die Datenquelle mit dem Namen **Quest One ActiveRoles 6.8.0-Berichtsdaten** aus.
3. Klicken Sie im rechten Bereich auf **Datenquelle ändern**.
4. Folgen Sie den Anweisungen des Assistenten.
5. Führen Sie folgende Schritte auf der Seite **Authentifizierungsmodus auswählen** im Assistenten aus:
   a) Geben Sie die SQL Server-Instanz an, auf der sich die Datenbank befindet, die die Berichtsdaten enthält.
   b) Wählen Sie die für die Verbindung zur Datenbank zu verwendende Authentifizierungsmethode aus. Geben Sie bei Bedarf Anmeldeinformationen für den Zugriff ein.
6. Wählen Sie auf der Seite **Datenbank auswählen** die Datenbank aus, die die Berichtsdaten enthält.
7. Stellen Sie auf der Seite **Produkte auswählen** sicher, dass das Kontrollkästchen **Quest One ActiveRoles 6.8.0.-Berichterstattungspaket** aktiviert ist.
8. Schließen Sie den Assistenten ab.

Generieren und Anzeigen eines Berichts

Sie können Quest One ActiveRoles-Berichte mit Hilfe von SSRS Report Manager oder dem Quest Knowledge Portal generieren und als Vorschau anzeigen. Dieser Abschnitt enthält grundlegende Anweisungen bezüglich der Verwendung von Report Manager oder des Knowledge Portals für diesen Zweck.

Die folgenden Anweisungen setzen voraus, dass Berichtsdaten mit Hilfe von Quest One ActiveRoles Collector vorbereitet wurden und dass die Datenquelle auf dem Berichtsserver so konfiguriert wurde, dass eine Verbindung mit der Datenbank besteht, in der die Berichtsdaten gespeichert sind.

Gehen Sie folgendermaßen vor, um einen Bericht mit Hilfe von SSRS Report Manager anzuzeigen:

1. Starten Sie SSRS Report Manager und rufen Sie die Seite **Inhalt** auf.
2. Klicken Sie auf der Seite **Inhalt** auf **QKP**.
3. Finden Sie einen Bericht, indem Sie die Ordner durchsuchen oder den Bericht anhand seines Namens suchen.

   *Durchsuchen Sie die Ordnerinhalte, indem Sie auf einen Ordnernamen oder auf ein Ordnersymbol auf der Seite **Inhalt** klicken. Suchen Sie nach einem Bericht, indem Sie den gesamten Berichtsnamen oder einen Teil des Namens in das Textfeld **Suchen nach** oben auf der Seite eingeben.*

4. Klicken Sie auf den Namen eines Berichts, um den Bericht anzuzeigen.

   Einige Berichte erfordern die Eingabe von Parameterwerten. Sie können auch Filter anwenden, um anzugeben, welche Daten der Bericht enthalten soll.

5. Klicken Sie auf die Schaltfläche „Bericht anzeigen“ oben auf der Seite.

Detaillierte Anweisungen bezüglich der Verwendung von Report Manager finden Sie in Microsoft SQL Server Books Online.

Gehen Sie folgendermaßen vor, um einen Bericht mit Hilfe von Quest Knowledge Portal anzuzeigen:

1. Klicken Sie im linken Bereich des Knowledge Portal-Fensters auf Berichte und suchen Sie dann einen **Bericht**, indem Sie Ordner durchsuchen.
2. Wählen Sie den Bericht im linken Bereich aus und klicken Sie dann auf **Bericht anzeigen** im rechten Bereich.

Nach der Erstellung wird der Bericht im Berichtsvorschaubereich angezeigt. Der Vorschaubereich umfasst eine Berichts-Symbolleiste, die über dem Bericht angezeigt wird, sodass Sie durch die Berichtsseiten blättern, eine Suche innerhalb eines Berichts ausführen oder den Bericht in einem anderen Format exportieren können.

Detaillierte Anweisungen bezüglich der Installation, Konfiguration und Verwendung von Quest Knowledge Portal finden Sie in der im Lieferumfang dieses Produkts enthaltenen Dokumentation.

Inhalt des Quest One ActiveRoles-Berichtserstattungspakets

Dieser Abschnitt enthält eine Liste der Berichte, die mit Hilfe von Quest One ActiveRoles Pack vorbereitet werden können. Die Liste ist in Unterabschnitte gegliedert. Die Überschrift jedes Unterabschnitts gibt den Pfad zu einem bestimmten Berichtsordner an, wobei sich die Berichte in dem Ordner befinden, der unter der Überschrift des Unterabschnitts aufgeführt ist.

Active Directory-Bewertung/Domänen/

- **Domänen-Zusammenfassung.** Erstellt eine Liste der Active Directory-Domänen in Ihrer Umgebung. Für jede Domäne sind die folgenden Informationen angegeben: Beschreibung, kanonischer Name, Funktionsebene, Erstellungsdatum und Zuletzt geändert sowie statistische Angaben zur Anzahl der Konten unterschiedlicher Typen in der Domäne.
- **Domänenvertrauensstellung.** Für jede Active Directory-Domäne werden die Domänen mit Domänenvertrauensstellung (vertrauenswürdige Domäne) und die Domänen, die der angegebenen Domäne vertrauen (vertrauende Domäne), aufgelistet.
- **Domänenkonto-SID-Auflösung.** Listet die Sicherheits-ID (SID) sowie den Objektnamen für jedes Sicherheitsprinzipalobjekt auf. Sicherheitsprinzipals sind Konten in Active Directory, denen Berechtigungen wie Benutzerkonten, Gruppen oder Computerkonten zugewiesen werden können. Active Directory weist jedem Sicherheitsprinzipalobjekt bei der Erstellung automatisch eine individuelle SID zu.

Active Directory-Bewertung/Benutzer/Kontoinformationen/

- **Benutzerkontoliste.** Listet die Benutzerkonten der Active Directory-Domäne in einer bestimmten Domäne oder einem bestimmten Container (Organisationseinheit) auf.
- **Benutzerkontooptionen.** Listet die Benutzerkonten der Active Directory-Domäne sowie Informationen über den Status der Kontooptionen wie beispielsweise „Benutzer muss Kennwort bei der nächsten Anmeldung ändern" und „Kennwort läuft nie ab" auf.
- **Kennwortalterinformationen.** Listet die Benutzerkonten der Active Directory-Domäne sowie Informationen zum Kennwortalter des Kontos auf. Das Kennwortalter für jedes Konto in der Liste wird mittels des Attributs pwdLastSet für das Konto berechnet. Die Kennwortalterinformationen helfen dabei, zu bestimmen, wann der Benutzer sein Kennwort das letzte Mal geändert hat.
- **Informationen über falsche Kennwörter.** Listet die Benutzerkonten der Active Directory-Domäne auf sowie Informationen über die Anzahl der Anmeldeversuche mit einem falschen Kennwort und das letzte Mal, als der Benutzer die Anmeldung mit einem falschen Kennwort versuchte.

Active Directory-Bewertung/Benutzer/Exchange 2000/2003/

- **Postfachinformationen nach Benutzern.** Listet die Benutzerkonten der Active Directory-Domäne auf sowie Informationen dazu, ob das Konto Postfach-fähig ist (über ein Exchange-Postfach verfügt). Hier können die Postfach-bezogenen Informationen detailliert eingesehen werden.
- **E-Mail-Übermittlungseinschränkungen.** Listet alle Postfach-fähigen (Exchange) Benutzerkonten auf sowie Informationen zu Zustellungsbeschränkungen wie die maximale Größe eingehender und ausgehender Nachrichten für dieses Postfach und von wem das Postfach E-Mails empfangen kann.
- **E-Mail-Übermittlungsoptionen.** Listet alle Postfach-fähigen (Exchange) Benutzerkonten auf sowie Informationen zu E-Mail-Übermittlungsoptionen wie wer zum Nachrichtenversand im Namen des Postfachbenutzers berechtigt ist, die Weiterleitungsadresse für dieses Postfach und die maximale Anzahl von Empfängern, an die der Postfachbenutzer eine Nachricht schicken kann.

Active Directory-Bewertung/Benutzer/Alte Konten/

- **Deaktivierte Benutzerkonten.** Listet die momentan deaktivierten Benutzerkonten der Active Directory-Domäne auf. Sie können jedes Konto detailliert einsehen.
- **Abgelaufene Benutzerkonten.** Listet Benutzerkonten der Active Directory-Domäne auf, die abgelaufen sind. Sie können jedes Konto detailliert einsehen.
- **Inaktive Benutzerkonten.** Listet Benutzerkonten der Active Directory-Domäne auf, bei denen innerhalb eines bestimmten Zeitraums keine Anmeldung mehr stattgefunden hat. Sie können jedes Konto detailliert einsehen.
- **Gesperrte Benutzerkonten.** Listet die Benutzerkonten der Active Directory-Domäne auf, die momentan aufgrund mehrerer fehlgeschlagener Anmeldeversuche gesperrt sind. Sie können jedes Konto detailliert einsehen.
- **Benutzerkonten mit abgelaufenem Kennwort.** Listet Benutzerkonten der Active Directory-Domäne auf, deren Kennwort abgelaufen ist. Sie können jedes Konto detailliert einsehen.
- **Deprovisionierte Benutzerkonten.** Listet die momentan von Quest One ActiveRoles deprovisionierten Benutzerkonten der Active Directory-Domäne auf. Sie können jedes Konto detailliert einsehen.
- **Alle eingestellten Benutzerkonten.** Listet die Benutzerkonten der Active Directory-Domäne auf, die aus verschiedenen Gründen ungenutzt sind, beispielsweise deaktivierte, abgelaufene, gesperrte, deprovisionierte Konten oder solche mit abgelaufenem Kennwort. Sie können jedes Konto detailliert einsehen.

Active Directory-Bewertung/Benutzer/Verschiedene Informationen/

- **Benutzer mit angegebenen Eigenschaften.** Listet die Benutzerkonten der Active Directory-Domäne auf, die über die von Ihnen angegebenen Eigenschaften verfügen. Sie können jedes Konto detailliert ansehen.
- **Benutzerprofilinformationen.** Listet die Benutzerkonten der Active Directory-Domäne auf sowie deren Profileinstellungen, wie den Pfad zum Benutzerprofil, den Namen des Anmeldeskripts und den Pfad zum Stammordner des Benutzers.
- **Vom Benutzer verwaltete Objekte.** Listet die Benutzerkonten der Active Directory-Domäne auf sowie Informationen zu deren verwalteten Objekten. Die Liste der verwalteten Objekte für das entsprechende Konto enthält diejenigen Objekte, bei denen unter „Verwaltet von" dieses Konto angegeben ist.
- **Persönliche Hierarchie.** Listet die Benutzerkonten der Active Directory-Domäne auf sowie Informationen zu ihrem Verwalter und Untergebenen. Die Verwalter-ID stammt aus den Verwaltereigenschaften des Kontos, die Liste der Untergebenen basiert auf der Eigenschaft „Direkte Berichte".

Active Directory-Bewertung/Gruppen/

- **Domänengruppenstatistik.** Listet die Anzahl der Gruppen in einer Active Directory-Domäne nach Gruppentyp (Sicherheit oder Distribution) und Gruppenausmaß (universell, global oder domänenspezifisch) auf. Hier können Sie alle Gruppen eines Typs und Ausmaßes anzeigen sowie detaillierte Informationen zu jeder Gruppe.
- **Gruppenliste mit Mitgliederstatistiken.** Listet die Gruppen in einer Active Directory-Domäne sowie Informationen zur Mitgliederanzahl jeder Gruppe auf. Sie können eine Mitgliederliste jeder Gruppe anzeigen.
- **Gruppenhierarchie.** Listet die in einer Active Directory-Domäne definierten Gruppen auf. Die Gruppenverschachtelung wird in einer Strukturansicht dargestellt. Sie können eine Liste der Mitgliedsgruppen in jeder Gruppe anzeigen und jede Gruppe im Detail ansehen.
- **Leere Gruppen.** Listet die in einer Active Directory-Domäne definierte Gruppen auf, die keine Mitglieder haben.

Active Directory-Bewertung/Gruppenmitgliedschaft/

- **Gruppenmitgliedschaft nach Gruppe.** Listet die Gruppenmitglieder jeder in einer Active Directory-Domain definierten Gruppe auf. Sie können die Liste so konfigurieren, dass nur ein bestimmter Mitgliedertyp (wie Benutzer, Computer oder Gruppe), nur direkte Mitglieder oder sowohl direkte Mitglieder als auch über Gruppenverschachtelung angehörige Mitglieder angezeigt werden.
- **Gruppenmitgliedschaft nach Benutzern.** Listet für jedes in einer Active Directory-Domäne definiertes Benutzerkonto auf, bei welchen Gruppen das Benutzerkonto Mitglied ist. Sie können die Liste so konfigurieren, dass nur Gruppen eines bestimmten Typs und Ausmaßes, nur Gruppen, bei denen der Benutzer ein direktes Mitglied ist oder sowohl Gruppen, in denen der Benutzer ein direktes Mitglied ist als auch solche, denen er über Gruppenverschachtelung angehört, angezeigt werden.
- **Benutzer mit administrativen Rechten für Domänen.** Listet für jede Active Directory-Domäne die Benutzerkonten auf, die der integrierten Administratorgruppe dieser Domain angehören, unabhängig davon ob sie ein direktes Mitglied sind oder anderen, in der Administratorgruppe eingebetteten Gruppen angehören. Sie können jedes aufgelistete Konto detailliert einsehen.

Active Directory-Bewertung/Organisationseinheiten/

- **Mitgliederstatistik nach Organisationseinheiten.** Gibt Informationen zur Anzahl der Objekte in jeder Organisationseinheit. Die Liste ist nach Objekttyp aufgegliedert, sodass Sie die Anzahl der Objekte jedes Typs sehen können, wie beispielsweise die Anzahl von Benutzern, Computern, Gruppen, Kontakten, Druckern und freigegebenen Ordnern. Durch Klicken einer Zahl in der Liste werden die von dieser Zahl dargestellten Objekte angezeigt.
- **Mitgliedschaft in Organisationseinheiten.** Listet für jede Organisationseinheit (Organizational Unit, OU) die in dieser OU enthaltenen Objekte auf. Der Bericht ist nach Objekttypen aufgegliedert, sodass Sie die Objekte jedes Typs in einer separaten Liste anzeigen können. Sie können Informationen zu den folgenden Objekten anzeigen: Benutzer, Computer, Gruppen, Kontakte, Drucker und freigegebene Ordner.
- **Hierarchie der Organisationseinheit.** Listet die in einer Active Directory-Domäne definierten Organisationseinheiten (OU) auf. Das Verhältnis der übergeordneten und untergeordneten Elemente der OU werden strukturiert dargestellt. Anhand dieses Berichts können Sie alle OUs bestimmen, die einer bestimmten OU entstammen und alle in dieser OU verwurzelten OUs anzeigen.

Active Directory-Bewertung/Andere Verzeichnisobjekte/

- **Active Directory-Objekteigenschaften.** Listet die Objekte auf, welche die von Ihnen angegebenen Bedingungen erfüllen. Für jedes Objekte werden Informationen zu den Eigenschaften angegeben, sodass Sie die anzuzeigenden Eigenschaften bestimmen können.
- **Computerkonten.** Listet alle in einer Domäne oder einem Container (Organisationseinheit) vorhandenen Computerkonten auf. Sie können diese Liste nach verschiedenen Kriterien wie Erstellungsdatum, Status (aktiviert oder deaktiviert) oder Betriebssystem der Computerkonten filtern.
- **Alle eingestellten Computerkonten.** Listet die Computerkonten der Active Directory-Domäne auf, die aus verschiedenen Gründen ungenutzt sind, beispielsweise deaktivierte, abgelaufene Konten oder solche an denen sich seit Langem keiner mehr angemeldet hat oder deren Kennwort abgelaufen ist. Sie können jedes Konto detailliert einsehen.

Active Directory-Bewertung/Mögliche Probleme/

- **Zyklische Gruppen.** Listet die Active Directory-Gruppen auf, die Mitglied bei sich selbst sind (sofern vorhanden). Anhand dieses Berichts können Sie feststellen, ob Ihre Active Directory-Domäne über Gruppen verfügt, die so eingestellt sind, dass sie bei sich selbst Mitglied sind (Gruppe A ist beispielsweise ein Mitglied von Gruppe B, die wiederum Mitglied von Gruppe A ist). Diese Konfiguration kann zu administrativen Problemen führen.

Quest One ActiveRoles-Verlaufsprotokoll/Active Directory-Verwaltung/

- **Benutzerattributverwaltung.** Listet die am Benutzerkonto der Active Directory-Domäne über Quest One ActiveRoles vorgenommenen Änderungen auf, sodass Sie feststellen können, wann und von wem einzelne Benutzereigenschaften geändert wurden und auf welche Werte die Eigenschaften eingestellt wurden. Sie können die Liste nach Änderungszeiträumen, den Namen der ändernden Personen und dem Namen der geänderten Eigenschaften filtern.
- **Verzeichnisverwaltung.** Listet die an Active Directory über Quest One ActiveRoles vorgenommen Änderungen auf, sodass Sie die Änderungen detailliert einsehen und feststellen können, wer wann welche Änderungen vorgenommen hat. Sie können verschiedene Bedingungen einstellen, um die Liste nach Objekttyp (wie Benutzer, Computer, Gruppe oder ein beliebiger anderer Objekttyp), Änderungskategorie (wie Erstellung, Bearbeitung oder Löschung von Objekten), geänderten Objekteigenschaften, Änderungszeitraum und Name der ändernden Person zu filtern.
- **Deprovisionierung von Benutzerkonten.** Listet die Benutzerkonten der Active Directory-Domäne auf, die über Quest One ActiveRoles deprovisioniert wurden, sodass Sie feststellen können, wer wann welche Benutzerkonten deprovisioniert hat. Sie können die Liste nach Zeiträumen, in denen Benutzerkonten deprovisioniert wurden, Name der Person, die Benutzerkonten deprovisioniert hat und Name und Ort des deprovisionierten Benutzerkontos filtern.

Quest One ActiveRoles-Verlaufsprotokoll/Dashboard/

- **Benutzerkontoverwaltung.** Hier können Sie einsehen, wie viele Operationen zur Benutzerkontoverwaltung innerhalb eines bestimmten Zeitraums stattgefunden haben. Die folgenden Operationstypen sind abgedeckt: (1) Erstellen; (2) Ändern (Eigenschaften ändern); (3) Zu Gruppen hinzufügen; (4) Aus Gruppen entfernen; (5) Anstelle aktueller Gruppenmitglieder hinzufügen; (6) Löschen. Sie können den gewünschten Zeitraum spezifizieren. Im Bericht wird für jeden Operationstyp ein eigenes Diagramm mit der Anzahl der zu einem bestimmten Zeitpunkt innerhalb dieses Zeitraums durchgeführten Operationen angezeigt.

Quest One ActiveRoles-Verlaufsprotokoll/Quest One ActiveRoles-Ereignisse/

- **Quest One ActiveRoles Startfehler.** Listet alle Fälle auf, in denen der Verwaltungsdienst von Quest One ActiveRoles nicht gestartet wurde sowie Informationen zur Fehlerursache. Sie können die Liste nach Zeiträumen, in denen Startfehler auftraten, filtern.
- **Quest One ActiveRoles Ereignisstatistik.** Dieser Bericht fasst die Quest One ActiveRoles-Ereignisse zusammen und gruppiert sie nach Datum (an dem die Ereignisse auftraten), nach Benutzer (der die Ereignisse auslöste), nach Computer (auf dem die Ereignisse protokolliert wurden) oder nach Ereigniskategorie. Sie können die Liste nach Zeitraum, Ereigniskategorie und Ereignis-ID filtern.

Quest One ActiveRoles-Verlaufsprotokoll/Quest One ActiveRoles-Konfigurationsänderungen/

- **Delegation der Kontrolle.** Listet die Zugriffsvorlagen von Quest One ActiveRoles auf, die zur Konfiguration der administrativen Berechtigungen in Quest One ActiveRoles angewendet werden. Für jede Zugriffsvorlage werden im Bericht die Objekte aufgelistet, mit denen die Zugriffsvorlage verknüpft ist. Außerdem wird angegeben, wann und von wem die Zugriffsvorlagenverknüpfung erstellt wurde. Sie können die Liste nach Name der Zugriffsvorlage, Name des Objekts, mit dem die Zugriffsvorlage verknüpft ist, Zeitraum, in dem die Verknüpfung erstellt wurde, und Name des Benutzers, der die Verknüpfung erstellt hat, filtern.
- **Richtlinienerzwingung.** Listet die Quest One ActiveRoles-Richtlinienobjekte auf, die zur Konfiguration der administrativen Richtlinie in Quest One ActiveRoles angewendet werden. Für jedes Richtlinienobjekt werden im Bericht die Objekte aufgelistet, mit denen das Richtlinienobjekt verknüpft ist. Außerdem wird angegeben, wann und von wem die Richtlinienobjektverknüpfung erstellt wurde. Sie können die Liste nach Name des Richtlinienobjekts, Name des Objekts, mit dem das Richtlinienobjekt verknüpft ist, Zeitraum, in dem die Verknüpfung erstellt wurde, und Name des Benutzers, der die Verknüpfung erstellt hat, filtern.

Quest One ActiveRoles-Verlaufsprotokoll/Quest One ActiveRoles-Arbeitsablauf/

- **Genehmigungen und Ablehnungen.** Listet über Quest One ActiveRoles gestellte Vorgangsanfragen auf, die während eines bestimmten Zeitraums genehmigt oder abgelehnt wurden. Sie können die von der genehmigenden Instanz ausgeführten Aktionen einsehen. Sie können die Liste nach Namen der Personen, die Anfragen genehmigt oder abgelehnt haben (genehmigende Instanz), Namen der Personen deren Anfragen genehmigt werden mussten (Initiator), Genehmigungsentscheidung (genehmigte oder abgelehnte Anfragen) und Name und Standort des Zielobjekts des Vorgangs filtern. Sie können die Liste nach genehmigender Instanz, Initiator oder Zielobjekt des Vorgangs ordnen.
- **Arbeitsablauf-Überwachung.** Listet Ereignisse auf, die spezifisch zum Quest One ActiveRoles-Arbeitsablauf gehören, und gruppiert diese nach der Operation, die den Arbeitsablauf angestoßen hat, oder nach Name des Arbeitsablaufs. Sie können so die Arbeitsablaufinstanzen überwachen. Im Bericht werden für jede Arbeitsablaufinstanz die Vorgangsanforderung, welche die Instanz gestartet hat, identifiziert, sowie Datum und Uhrzeit des Instanzenstarts, die Person, welche die Vorgangsanforderung einreichte (Initiator), das Zielobjekt der Operation, der zur Anforderungsdurchführung vorgesehene Server sowie alle Ereignisse, die während der Arbeitsablaufinstanz stattgefunden haben. Sie können die Liste der Arbeitsablaufinstanzen nach verschiedenen Parametern wie Datum und Uhrzeit, Vorgangs-ID, Arbeitsablaufname, Vorgangsinitiator, Zielobjekt, Ereigniskategorie und Ereignis-ID filtern.

Administratorfunktionen/

- **Zugriffsvorlagenberechtigungen.** Listet alle Quest One ActiveRoles-Zugriffsvorlagen auf, sodass Sie jede Zugriffsvorlage im Detail einsehen können. Sie können den Namen, Standort und die Beschreibung der Zugriffsvorlage sowie alle Berechtigungseinträge der Zugriffsvorlage ansehen.
- **Zugriffsvorlagen-Zusammenfassung.** Listet alle Quest One ActiveRoles-Zugriffsvorlagen sowie quantitative Informationen zu den Zugriffsvorlagenverknüpfungen auf. Sie können im Bericht für jede Zugriffsvorlage die Anzahl der Verknüpfungen bestimmen, die die Zugriffsvorlage verwenden, sowie die Anzahl der Objekte (Trustees und Container), auf die die Zugriffsvorlage verweist.
- **Mit verwalteten Einheiten verknüpfte Zugriffsvorlagen.** Listet alle Quest One ActiveRoles-Zugriffsvorlagen auf, die mit verwalteten Einheiten von Quest One ActiveRoles verknüpft sind. Identifiziert den Namen, Standort und die Beschreibung jeder Zugriffsvorlage sowie den vollqualifizierten Namen jeder verwalteten Einheit, mit der die Zugriffsvorlage verknüpft ist. Sie können die Liste erweitern, sodass sie sowohl verwaltete Einheiten, mit denen die Zugriffsvorlage verknüpft ist, als auch verwaltete Einheiten, die durch Berechtigungsvererbung von der Zugriffsvorlage beeinflusst werden, beinhaltet.
- **Mit Organisationseinheiten verknüpfte Zugriffsvorlagen.** Listet alle Quest One ActiveRoles-Zugriffsvorlagen auf, die mit Organisationseinheiten von Active Directory verknüpft sind. Identifiziert den Namen, Standort und die Beschreibung jeder Zugriffsvorlage sowie den vollqualifizierten Namen jeder Organisationseinheit, mit der die Zugriffsvorlage verknüpft ist. Sie können die Liste erweitern, sodass sowohl Organisationseinheiten, mit denen die Zugriffsvorlage verknüpft ist, als auch Organisationseinheiten, die durch Berechtigungsvererbung von der Zugriffsvorlage beeinflusst werden, angezeigt werden.
- **Delegation der Kontrolle nach Objekten.** Listet Active Directory-Objekte auf, die mit Quest One ActiveRoles-Zugriffsvorlagen verknüpft sind. Identifiziert den Namen, Standort und die Beschreibung jedes Objekts sowie den Namen jeder mit diesem Objekt verknüpften Zugriffsvorlage und den Sicherheitsprinzipal (Trustee), dessen administrative Berechtigungen durch direkte Zuordnung von dieser Verknüpfung festgelegt werden (ohne Berücksichtigung der Zugriffsvererbung).
- **Delegation der Kontrolle nach Objekten (mit Gruppenhierarchie).** Listet Active Directory-Objekte auf, die mit Quest One ActiveRoles-Zugriffsvorlagen verknüpft sind. Identifiziert den Namen, Standort und die Beschreibung jedes Objekts sowie den Namen jeder mit diesem Objekt verknüpften Zugriffsvorlage und die Sicherheitsprinzipale (Trustees), deren administrative Berechtigungen durch direkte Zuordnung oder Gruppenmitgliedschaften von dieser Verknüpfung festgelegt werden.
- **Delegation der Kontrolle nach Trustee.** Listet die Sicherheitsprinzipale (Trustees) von Active Directory auf, die administrative Berechtigungen durch die Anwendung von Quest One ActiveRoles.Zugriffsvorlagen haben. Identifiziert den Namen jedes Trustees sowie den Namen jeder Zugriffsvorlage, die die administrativen Berechtigungen des Trustees in Quest One ActiveRoles festlegt, sowie den Namen des Containers oder Blattobjekts, mit dem die Zugriffsvorlage verknüpft ist, was dazu führt, dass der Trustee über administrative Berechtigungen für den Container oder das Blattobjekt verfügt.
- **Delegation der Kontrolle nach Trustee (mit Containerhierarchie).** Listet Sicherheitsprinzipale (Trustees) auf, die administrative Berechtigungen durch die Anwendung von Quest One ActiveRoles-Zugriffsvorlagen haben, und gibt detaillierte Informationen zu sicherbaren Objekten und Containern, zu denen der Trustee administrative Berechtigungen hat, und den Zugriffsvorlagen, welche die Berechtigungen des Trustees festlegen. Sie können die Liste der Trustees nach verschiedenen Parametern filtern, wie Name und Typ des Trustees, sicherbares Objekt oder Name und Typ des Containers, Name und Typ der Zugriffsvorlage, Name und Typ der Berechtigung und Typ der Berechtigungsvererbung.

Verwaltete Einheiten/

- **Mitglieder der verwalteten Einheit.** Listet alle verwalteten Einheiten von Quest One ActiveRoles sowie deren Mitglieder auf. Der Name, Pfad und die Beschreibung jeder verwalteten Einheit sowie der Name, Typ und die Beschreibung jedes Objekts in der verwalteten Einheit werden angegeben.
- **Mitgliedschaftsregeln der verwalteten Einheit.** Listet alle verwalteten Einheiten von Quest One ActiveRoles sowie deren Mitgliedschaftsregeln auf. Der Name, Pfad und die Beschreibung jeder verwalteten Einheit sowie die Regeln, welche die in die verwaltete Einheit einzuschließen oder auszuschließenden Objekte festlegen, werden angegeben.
- **Verwaltete Einheit - Zusammenfassung.** Listet alle verwalteten Einheiten von Quest One ActiveRoles auf sowie quantitative Informationen zu den Mitgliedern der verwalteten Einheit, Mitgliedschaftsregeln, Trustees und Richtlinien. Die Mitgliederanzahl und Mitgliedschaftsregeln jeder verwalteten Einheit sowie die Anzahl der Sicherheitsprinzipale (Trustees) mit administrativen Berechtigungen für diese verwaltete Einheit und die Anzahl der die verwaltete Einheit betreffenden Quest One ActiveRoles-Richtlinienobjekte werden angegeben.
- **Von der Richtlinie betroffene verwaltete Einheiten.** Listet die verwalteten Einheiten von Quest One ActiveRoles auf, die von den Quest One ActiveRoles-Richtlinienobjekten betroffen sind, entweder durch ein mit der verwalteten Einheit selbst verknüpftes Richtlinienobjekt oder eine andere verwaltete Einheit, welche die fragliche verwaltete Einheit beinhaltet. Für jede verwaltete Einheit werden Name und Beschreibung jedes Richtlinienobjekts, welches die verwaltete Einheit beeinflusst, sowie der Container oder die verwaltete Einheit, von wo der Richtlinieneffekt vererbt wurde, angegeben.
- **Verwaltete Einheiten mit delegierter Kontrolle.** Listet verwaltete Einheiten von Quest One ActiveRoles auf, an die administrative Kontrolle delegiert wurde. Dies kann durch die Anwendung von Quest One ActiveRoles-Zugriffsvorlagen auf die verwaltete Einheit selber (direkte Berechtigungen) oder auf einen Container oder eine andere verwaltete Einheit, welche die fragliche verwaltete Einheit beinhaltet (vererbte Berechtigungen) geschehen. Für jede verwaltete Einheit werden die Sicherheitsprinzipale (Trustees) angegeben, an welche die administrative Kontrolle delegiert wurde, sowie die Zugriffsvorlagen, welche die administrativen Berechtigungen festlegen und die Tatsache, ob es sich um direkte oder vererbte Berechtigungen handelt.

Richtlinienobjekte/

- **Einstellungen für die Auswertung der verknüpften Eigenschaft.** Listet Objekteigenschaften auf, die der Kontrolle einer in Quest One ActiveRoles definierten Richtlinie zur Erzeugung und Validierung von Eigenschaften unterliegen. Für jede Eigenschaft werden die Objektklassen mit dieser Eigenschaft aufgelistet, die die Eigenschaft beeinflussenden Richtlinienobjekte, der mit dem Richtlinienobjekt verknüpfte Container sowie die Richtlinienbedingungen. Der Bericht beinhaltet nur Container, die direkt mit den Richtlinienobjekten verknüpft sind. Richtlinienvererbung wird nicht berücksichtigt. Sie können die Liste der Eigenschaften nach verschiedenen Parametern filtern, wie beispielsweise Name der Eigenschaft, Name der Objektklasse, Name des Containers und Name des Richtlinienobjekts.
- **Einstellungen für die Auswertung der verknüpften Eigenschaft (mit Vererbung).** Listet Objekte sowie deren Eigenschaften auf, die der Kontrolle einer in Quest One ActiveRoles definierten Richtlinie zur Erzeugung und Validierung von Eigenschaften unterliegen. Die Objekte in diesem Bericht sind möglicherweise mit einem Richtlinienobjekt (direkte Richtlinie) oder Container verknüpft, der das Objekt enthält (vererbte Richtlinie). Im Bericht werden die Objekte nach Eigenschaften gruppiert. Im Bericht werden für jede Eigenschaft die Objekte, welche diese Eigenschaft besitzen, aufgelistet und die Richtlinienobjekte und Richtlinienbedingungen angegeben, welche jedes der aufgelisteten Objekte beeinflussen. Es wird angegeben, ob es sich um eine direkte oder eine vererbte Richtlinie handelt. Sie können die Liste der Eigenschaften und Objekteigenschaften nach verschiedenen Parametern filtern, wie beispielsweise Name der Eigenschaft, Name und Typ des Objekts und Name des Richtlinienobjekts.

- **Einstellungen für das verknüpfte Skript (mit Vererbung).** Listet die Objekte auf, die der Kontrolle einer in Quest One ActiveRoles definierten skriptbasierten Richtlinie (Skriptausführung) unterliegen. Die Objekte in diesem Bericht sind möglicherweise mit Richtlinienobjekten (direkter Richtlinieneffekt) oder mit einem Container, der das Objekt enthält (vererbter Richtlinieneffekt), verknüpft. Im Bericht werden die skriptbasierten Richtlinienobjekte identifiziert, welche jedes der aufgelisteten Objekte beeinflussen, sowie der Ursprung des Richtlinieneffekts (direkt oder vererbt). Sie können die Liste der Objekte nach verschiedenen Parametern filtern, wie beispielsweise Name des Objekts, Name der Objektklasse und Name des Richtlinienobjekts.
- **Richtlinienobjektreferenzen.** Listet Quest One ActiveRoles-Richtlinienobjekte auf, die auf jeden Container und jede verwaltete Einheit angewendet werden (Verknüpfung). Für jedes Richtlinienobjekt werden der Name, die Beschreibung und Kategorie (Provisionierung oder Deprovisionierung) angegeben, sowie eine Liste der Container, mit denen das Richtlinienobjekt verknüpft ist. Sie können die Liste nach Namen der Richtlinienobjekte, Container oder Name der verwalteten Einheit sowie der Kategorie des Richtlinienobjekts filtern.
- **Richtlinienobjekteinstellungen.** Listet die Quest One ActiveRoles-Richtlinienobjekte mit deren Richtlinieneinträgen auf. Für jedes Richtlinienobjekt werden detaillierte Informationen zu allen im Richtlinienobjekt definierten Richtlinien angegeben. Sie können die Liste nach Namen des Richtlinienobjekts, Richtlinientyp und Name des Richtlinieneintrags filtern.
- **Richtlinienobjekt – Zusammenfassung.** Listet die Quest One ActiveRoles-Richtlinienobjekte mit folgenden Informationen zu jedem Richtlinienobjekt auf: Name, Typ (Provisionierung oder Deprovisionierung), Anzahl der Verzeichnisobjekte, mit denen das Richtlinienobjekt verknüpft ist (Anzahl Referenzen), Gesamtsumme der im Richtlinienobjekt definierten einzelnen Richtlinien (Anzahl Einträge), Anzahl der Richtlinien jedes Typs im Richtlinienobjekt.
- **Richtlinienobjekte mit sicherbaren Objekten.** Listet alle Quest One ActiveRoles-Richtlinienobjekte mit den von jedem Richtlinienobjekt betroffenen Verzeichnisobjekten auf. Ein Verzeichnisobjekt in diesem Bericht kann mit einem Richtlinienobjekt (direkter Richtlinieneffekt) oder Container, der das Objekt enthält (vererbter Richtlinieneffekt), verknüpft sein. Für jedes von einem Richtlinienobjekt betroffene Verzeichnisobjekt werden im Bericht der kanonische Name, Typ und die Beschreibung des Objekts genannt und die Angabe, ob der Richtlinieneffekt direkt oder vererbt ist. Sie können die Liste nach Name des Richtlinienobjekts, Richtlinientyp und Name und Typ des Verzeichnisobjekts filtern.
- **Sicherbare Objekte (mit Vererbung).** Listet Verzeichnisobjekte auf, die von Quest One ActiveRoles-Richtlinienobjekten betroffen sind. Für jedes Verzeichnisobjekt werden die mit dem Verzeichnisobjekt selbst (direkter Richtlinieneffekt) oder die mit einem Container, der das Verzeichnisobjekt enthält (vererbter Richtlinieneffekt), verknüpften Richtlinienobjekte angegeben. Für jedes Richtlinienobjekt, welches das fragliche Verzeichnisobjekt beeinflusst, werden im Bericht der Name, Pfad, die Beschreibung und Richtlinieneinträge des Richtlinienobjekts aufgelistete sowie die Tatsache, ob es sich um einen direkten oder indirekten Richtlinieneffekt handelt. Sie können die Liste nach Name und Typ des Verzeichnisobjekts, Name und Typ des Richtlinienobjekts und Name des Richtlinieneintrags filtern.

Richtlinienkonformität/

- **Objekte, die gegen die Richtlinienregeln verstoßen.** Listet Verzeichnisobjekte und deren Eigenschaften auf, die gegen die Richtlinien in Quest One ActiveRoles-Richtlinienobjekten verstoßen. Für jedes Verzeichnisobjekt werden Objektname, übergeordneter Container, Typ und Beschreibung angegeben und welche Eigenschaften gegen Richtlinienregeln verstoßen und welche Richtlinienobjekte die verletzten Richtlinienregeln definieren.
- **Verletzte Richtlinienregeln.** Listet Richtlinienobjekte von Quest One ActiveRoles auf, deren Richtlinienregeln durch bestimmte Verzeichnisobjekte verletzt wurden. Für jedes Richtlinienobjekt werden die in diesem Richtlinienobjekt definierten Richtlinien angegeben und für jede einzelne Richtlinie werden Informationen zu Verzeichnisobjekten und deren Eigenschaften, die gegen diese Richtlinie verstoßen, aufgelistet.

11

Verwaltungsverlauf

- Beschreibung des Verwaltungsverlaufs
- Konfiguration des Verwaltungsverlaufs
- Untersuchen des Änderungsverlaufs
- Untersuchen von Benutzeraktivitäten

Beschreibung des Verwaltungsverlaufs

Die Funktion für den Verwaltungsverlauf stellt Informationen dazu bereit, welcher Benutzer zu welchem Zeitpunkt welche Verwaltungsaufgaben für Active Directory mit Hilfe von Quest One ActiveRoles ausgeführt hat.

Diese Funktion stellt ein gut verständliches Protokoll bereit, das die an einem bestimmten Objekt vorgenommenen Änderungen dokumentiert, wie etwa an einem Benutzer- oder Gruppenobjekt. Das Protokoll enthält detaillierte Einträge zu den ausgeführten Aktionen, zum Erfolg oder Fehler jeder Aktion sowie zu den geänderten Attributen.

Mit Hilfe des Verwaltungsverlaufs können Sie Folgendes untersuchen:

- **Änderungsverlauf.** Informationen zu Änderungen an Verzeichnisdaten, die über Quest One ActiveRoles vorgenommen wurden.
- **Benutzeraktivität.** Informationen zu Verwaltungsaktionen, die ein bestimmter Benutzer ausgeführt hat.

Sowohl „Änderungsverlauf" als auch „Benutzeraktivität" verwenden dieselbe Informationsquelle – das Verwaltungsverlaufsprotokoll, das auch als Änderungsverfolgungsprotokoll bezeichnet wird. Die Konfigurationseinstellungen des Änderungsverfolgungsprotokolls werden weiter unten in diesem Kapitel beschrieben (siehe „Konfiguration des Verwaltungsverlaufs").

Quest One ActiveRoles umfasst auch Berichte, um den Verwaltungsverlauf durch die Erfassung und Analyse von Ereignisprotokolleinträgen zu untersuchen (siehe „Berichterstattung von Quest One ActiveRoles" weiter oben in diesem Dokument). Das Abrufen und Konsolidieren von Datensätzen aus dem Ereignisprotokoll kann zeitaufwändig und ineffizient sein.

Überlegungen und optimale Vorgehensweisen

In diesem Abschnitt werden Informationen und Empfehlungen bereitgestellt, die Sie berücksichtigen sollten, wenn Sie beabsichtigen, die Funktion für den Verwaltungsverlauf zu verwenden.

Diese Funktion soll Ihnen ermöglichen, umgehend zu untersuchen, welche Änderungen vor kurzem an den Verzeichnisdaten vorgenommen wurden, und zwar wann und von welchem Benutzer. Diese Funktion ist prinzipiell weder für die Überwachung von Datenänderungen bestimmt noch für die Untersuchung großer Mengen von Datenänderungen, die in einem langen Zeitraum aufgetreten sind.

Deshalb stellt Quest One ActiveRoles zusätzlich zu der Funktion für den Verwaltungsverlauf eine Folge von Berichten für die Nachverfolgung und Überwachung von Änderungen dar. Diese gehört zum Berichterstattungspaket von Quest One ActiveRoles. Außerdem ist das InTrust Knowledge Pack erhältlich, mit dem Quest One ActiveRoles sehr große Protokolle der Änderungsnachverfolgung verarbeiten und analysieren kann. Das Produkt InTrust wird separat von Quest One ActiveRoles verkauft.

Jede dieser drei Optionen (Verwaltungsverlauf, Berichterstattungspaket und Knowledge Pack) hat eigene Vorteile und Grenzen. Befolgen Sie die Empfehlungen in diesem Abschnitt, um die Option auszuwählen, die Ihren Anforderungen am besten entspricht.

Mit der Funktion für den Verwaltungsverlauf können Sie Änderungen untersuchen, die mit Quest One ActiveRoles an den Verzeichnisdaten vorgenommen wurden. Diese Funktion soll Ihnen helfen, die folgenden häufigen Fragen zu beantworten:

- Wer hat die letzten Änderungen an einem bestimmten Benutzer- oder Gruppenobjekt vorgenommen?
- Wer hat ein bestimmtes Benutzer- oder Gruppenobjekt in den letzten X Tagen geändert?

- Welche Änderungen wurde gestern Abend (gestern, vorgestern) an einem bestimmten Benutzerobjekt vorgenommen?
- Wurden geplante Änderungen an einem bestimmten Benutzer- oder Gruppenobjekt wirklich ausgeführt?
- Welche Objekte hat ein bestimmter delegierter Administrator in den letzten X Tagen geändert?

Sie können sofort auf den Verwaltungsverlauf zugreifen, wenn Sie ein Problem schnell untersuchen oder behandeln möchten, das aus ungeeigneten Änderungen von Verzeichnisdaten resultiert.

Die Funktion für den Verwaltungsverlauf schließt ein ausschließlich für sie verwendetes Repository ein, in dem Informationen zu Datenänderungen gespeichert werden. Dieses Repository wird als Verfolgungsprotokoll bezeichnet. Außerdem schließt sie eine spezielle grafische Benutzeroberfläche ein, über die Sie Informationen aus dem Repository abrufen und anzeigen können. Es sind keine zusätzlichen Aktionen erforderlich, wie etwa das Sammeln oder Konsolidieren von Informationen, um Verwaltungsverlaufs-Ergebnisse anhand des Verfolgungsprotokolls zu erstellen.

Die Vorteile der Funktion für den Verwaltungsverlauf bringen jedoch auch einige Einschränkungen mit sich. Bevor Sie die Funktion für den Verwaltungsverlauf verwenden, sollten Sie die folgenden empfohlenen optimalen Vorgehensweisen sowie Grenzen dieser Funktion überdenken.

Das Verfolgungsprotokoll ist in gewisser Weise unvollständig, da es keine Datenänderungen widerspiegelt, die von bestimmten Richtlinien gemacht werden, z.B von der Richtlinie „Automatische Bereitstellung der Gruppenmitgliedschaft". Wenn eine solche Richtlinie Benutzer zu Gruppen hinzufügt oder daraus entfernt, fehlen Informationen zu diesen Richtlinienaktionen im Protokoll und somit auch in den Verwaltungsverlaufs-Ergebnissen. Wenn Sie Informationen zu allen Datenänderungen benötigen, auch zu denen, die durch Richtlinienaktionen ausgelöst wurden, sollten Sie Nachverfolgungsberichte für Änderungen verwenden. Diese werden weiter unten in diesem Abschnitt diskutiert.

Ein weiterer Faktor, den Sie beachten sollten, ist die Größe des Verfolgungsprotokolls. Um sicherzustellen, dass das Protokoll für alle Verwaltungsdienste in Echtzeit aktualisiert wird, wird es normalerweise in der Konfigurationsdatenbank von Quest One ActiveRoles gespeichert. Diese führt zu einer Begrenzung der Protokollgröße.

Standardmäßig ist das Verfolgungsprotokoll so konfiguriert, dass nur Informationen zu Änderungen in den letzten 30 Tagen gespeichert sind. Wenn Sie diese Einstellung erhöhen, lassen Sie Vorsicht walten; andernfalls können die folgenden Probleme auftreten:

- Eine übermäßige Erhöhung der Protokollgröße erhöht den Zeitaufwand für das Erstellen und Anzeigen von Änderungsverlauf- und Benutzeraktivitätsergebnissen erheblich.
- Wenn das Protokoll vergrößert wird, steigt die Größe der Konfigurationsdatenbank mit. Dies erhöht die zum Sichern und Wiederherstellen der Datenbank erforderliche Zeit beträchtlich und verursacht hohen Netzwerk-Datenverkehr bei der Replikation der Datenbank, wenn Sie der Quest One ActiveRoles-Replikationsgruppe einen weiteren Verwaltungsdienst hinzufügen.
- Auf der grafischen Benutzeroberfläche können umfangreiche Verwaltungsverlaufs-Ergebnisse nicht überschaubar dargestellt werden. Da keine Filter- oder Seitenumbruchsfunktionen vorhanden sind, kann es unpraktisch und schwierig sein, die Ergebnisse strukturiert durchzusehen.

Um diese Einschränkungen zu überwinden, stellt Ihnen Quest One ActiveRoles ein anderes Hilfsmittel für die Überwachung von Änderungen bereit, die Nachverfolgungsberichte für Änderungen. Diese sind Teil des Berichterstattungspakets von Quest One ActiveRoles. Diese Berichte sollen Ihnen helfen, die folgenden Fragen zu beantworten:

- Welche Verwaltungsaufgaben wurden in einem bestimmten Zeitraum für ein bestimmtes Objekt ausgeführt?
- Welche Verwaltungsaufgaben wurden für ein bestimmtes Objekt während seiner gesamten Lebensdauer ausgeführt?
- Wann wurde ein bestimmtes Attribut eines bestimmten Objekts geändert?

Für die Arbeit mit Berichten bietet Quest One ActiveRoles eine erweiterte Berichterstattungslösung. Sie können Berichte mit umfangreichen Daten leicht verwalten: Konfigurieren Sie Filter und wenden Sie diese an, durchsuchen Sie die einzelnen Seiten und exportieren Sie Berichte in einer Vielzahl von Formaten.

Diese Berichte basieren auf Daten, die aus Ereignisprotokollen gesammelt werden. Auf jedem Computer mit dem Verwaltungsdienst wird ein separates Protokoll gespeichert. Jedes dieser Protokolle enthält nur Ereignisse, die der jeweilige Verwaltungsdienst generiert hat. Daher müssen Sie zum Verwenden von Berichten zunächst Ereignisse aus allen Ereignisprotokollen konsolidieren, sodass sie ein vollständiges Prüfprotokoll bilden.

Die Konsolidierung der Ereignisse, die als Datensammlungsprozess bezeichnet wird, wird von einer separaten Komponente von Quest One ActiveRoles ausgeführt, dem Collector. Mit dem Assistenten „Collector" können Sie Datensammlungsaufträge konfigurieren und ausführen sowie regelmäßige Ausführungen für sie planen.

Die wesentliche Einschränkung bei Nachverfolgungsberichten für Änderungen wird dadurch bedingt, dass Informationen in einer separaten Datenbank gesammelt und konsolidiert werden müssen, bevor Sie die Berichte vorbereiten können. Der Datensammlungsprozess weist folgende Nachteile auf:

- Der Datensammlungsvorgang kann sehr lange dauern, und die Datenbank kann inakzeptabel vergrößert werden, wenn Sie alle Ereignisse sammeln, die während eines langen Zeitraums in einer großen Umgebung aufgetreten sind.
- Daten können nicht über langsame WAN-Links gesammelt werden. Diese Einschränkung ist durch die Komponente von Quest One ActiveRoles bedingt, die Daten für die Berichterstattung sammelt.

Wenn Sie an diese Grenzen stoßen, können Sie das InTrust Knowledge Pack für Quest One ActiveRoles verwenden, um Ereignisprotokolle von Computern, auf denen der Verwaltungsdienst ausgeführt wird, zu konsolidieren und zu analysieren. Mit dem Knowledge Pack können sehr umfangreiche Nachverfolgungsdaten gespeichert, verwaltet und analysiert werden. Dieses Produkt verwendet komplexe Techniken, um Informationen aus Ereignisprotokollen zu sammeln und zu konsolidieren, sogar über langsame WAN-Verbindungen.

Konfiguration des Verwaltungsverlaufs

Die Konfiguration des Verwaltungsverlaufs umfasst die folgenden Elemente:

- **Richtlinie für die Änderungsnachverfolgung.** Stellt zum Verlauf der Änderungen an Verzeichnisobjekten gehörende Daten zusammen legt fest, welche Änderungen in Berichte über den Änderungsverlauf und über Benutzeraktivitäten aufgenommen werden.
- **Konfiguration des Verfolgungsprotokolls ändern.** Gibt an, wie viele Änderungsanforderungen im Protokoll gespeichert werden sollen.
- **Replikation von Verwaltungsverlaufsdaten.** Gibt an, ob Verwaltungsverlaufsdaten zwischen Verwaltungsdiensten, die verschiedene Datenbanken verwenden, synchronisiert werden soll oder nicht.

In den folgenden Abschnitten werden alle diesen Elemente ausführlich beschrieben.

Richtlinie für die Änderungsnachverfolgung

Das Verhalten der Verwaltungsverlaufsfunktion wird von der Richtlinie definiert, die im integrierten Richtlinienobjekt **Built-in Policy – Change Tracking definiert ist**. Die Richtlinie bestimmt die Objekttypen und -Eigenschaften, für die Informationen zum Verwaltungsverlauf gesammelt werden sollen.

Um die Richtlinie anzuzeigen oder zu ändern, zeigen Sie das Dialogfeld **Eigenschaften** für das Richtlinienobjekt **Built-in Policy – Change Tracking** an (dies befindet sich im Container **Configuration/Policies/Administration/Builtin**), öffnen Sie die Registerkarte **Richtlinien**, wählen Sie die Richtlinie aus und klicken Sie auf **Anzeigen/Bearbeiten**. Nun wird das Dialogfeld **Richtlinieneigenschaften** angezeigt. Unter **Objekttypen und -eigenschaften** in diesem Dialogfeld werden die Objekttypen und -eigenschaften aufgelistet, die in den Verwaltungsverlauf eingeschlossen werden. Jeder Eintrag in der Liste schließt die folgenden Informationen ein:

- **Objekttyp.** Wenn ein Objekt dieses Typs über Quest One ActiveRoles geändert wird, werden Informationen zu dieser Aktion im Änderungsverfolgungsprotokoll aufgezeichnet, sofern die Änderung sich auf eine in der Spalte **Eigenschaften** angegebene Eigenschaft auswirkt.
- **Eigenschaften.** Informationen über Änderungen an diesen Eigenschaften werden im Änderungsverfolgungsprotokoll aufgezeichnet.

Sie können die Liste auf der Registerkarte mit Hilfe der Schaltflächen unter der Liste wie folgt verwalten:

- **Hinzufügen.** Zeigt das Dialogfeld an, in dem Sie den Objekttyp und die Eigenschaften anzeigen können, die Sie in den Verwaltungsverlauf einschließen möchten. Sie können entweder einzelne oder alle Eigenschaften auswählen.
- **Entfernen.** Löscht die ausgewählten Einträge aus der Liste.
- **Anzeigen/Bearbeiten.** Zeigt das Dialogfeld an, in dem Sie die Eigenschaften für den ausgewählten Listeneintrag anzeigen und ändern können.

Konfiguration des Verfolgungsprotokolls ändern

Eine weitere Konfigurationseinstellung für den Verwaltungsverlauf bestimmt die Größe des Verfolgungsprotokolls. In dem Protokoll werden Informationen zu Anforderungen zur Änderung von Verzeichnisdaten gespeichert, ein Datensatz pro Anforderung. Jeder Datensatz enthält Informationen zu den Änderungen an einem bestimmten Objekt, die gemäß einer bestimmten Änderungsanforderung vorgenommen wurden.

Sie können die Maximalanzahl von Datensätzen konfigurieren, indem Sie Verwaltungsfunktionen für Eigenschaften des Objekts **Konfiguration des Verfolgungsprotokolls ändern** verwenden. Dieses befindet sich im Container **Configuration/Server Configuration**.

Auf der Registerkarte **Protokolleinstellungen** im Dialogfeld **Eigenschaften** können Sie eine der folgenden Optionen auswählen:

- **Alle Anfragen in den letzten** *Anzahl* **Tage.** Informationen über Änderungsanforderungen werden in das Protokoll geschrieben, sodass neue Anforderung die Anforderungen ersetzen, die älter als die angegebene Anzahl von Tagen sind.
- **Diese Zahl jüngster Anfragen.** Im Protokoll werden nicht mehr Änderungsanforderungen wie angegeben gespeichert. Wenn der Grenzwert erreicht ist, ersetzt jede neue Anforderung zur Änderung von Verzeichnisdaten die älteste Anforderung im Protokoll.
- **Diese Zahl jüngster Anfragen je Objekt.** Für jedes Objekt werden im Protokoll höchstens so viele Änderungsanforderungen gespeichert wie angegeben. Wenn der Grenzwert für ein bestimmtes Objekt erreicht ist, ersetzt jede neue Anforderung zur Änderung des Objekts die älteste, mit diesem Objekt in Verbindung stehende Anforderung. Die Gesamtzahl der Anforderungen hängt von der Anzahl der Objekte ab, die über Quest One ActiveRoles geändert werden.

Standardmäßig ist das Verfolgungsprotokoll so konfiguriert, dass Informationen zu Anforderungen in den letzten 30 Tagen gespeichert sind. Die Informationen über die Änderungsanforderungen werden in das Protokoll geschrieben, sodass neue Anforderungen solche Anforderungen ersetzen, die älter als 30 Tage sind. Wenn Sie diese Zahl erhöhen, lassen Sie Vorsicht walten. Wenn Sie diese Zahl deutlich erhöhen, wird auch das Protokoll umfangreicher. Wenn Sie beabsichtigen, diese Einstellung zu ändern, sollten Sie zunächst den Abschnitt „Überlegungen und optimale Vorgehensweisen" weiter oben in diesem Kapitel lesen.

Das Verfolgungsprotokoll wird als Informationsquelle für den Änderungsverlauf und den Verlauf zur Benutzeraktivität verwendet. Der Umfang der im Protokoll gespeicherten Anforderungen bestimmt den Wartezeitraum für den Änderungsverlauf sowie für die Benutzeraktivität.

Auf der Registerkarte **Protokolleintragsgröße** stehen Ihnen Optionen zur Auswahl, die es Ihnen ermöglichen, die Größe des Änderungsverfolgungsprotokolls zu reduzieren, indem detaillierte Informationen über eine begrenzte Anzahl von Änderungsanforderungen protokolliert werden. Dabei werden nur Basisinformationen über die anderen protokollierten Änderungsanforderungen vorliegen und solche, die in den Berichten enthalten sind. Wenn der Protokolleintrag einer bestimmten Änderungsanforderung detaillierte Informationen enthält, dann bietet der Bericht zu dieser Anforderung Informationen zu allen von Quest One ActiveRoles während der Verarbeitung der Anforderung vorgenommenen Änderungen sowie zu allen angewandten Richtlinien und durchgeführten Arbeitsabläufen. Andernfalls enthält der Bericht nur Informationen zu den in Übereinstimmung mit der Anforderung an den Objekteigenschaften durchgeführten Änderungen. Obwohl die Speicherung nur der grundlegenden Protokolleinträge zu weniger Details in den Berichten führt, kann dies zu einer beträchtlichen Verringerung der Größe der Verwaltungsverlaufsdatenbank führen. Die folgenden Optionen sind verfügbar:

- **Alle Anforderungen.** Das Änderungsverfolgungsprotokoll enthält detaillierte Informationen zu allen im Protokoll gespeicherten Anforderungen.
- **Anfragen in den letzten** *Anzahl* **Tage.** Detaillierte Informationen zu Anforderungen werden in das Protokoll geschrieben, so dass neue Anforderungen mit ausführlichen Informationen diejenigen ersetzen, die älter sind als die angegebene Anzahl von Tagen.
- **Diese Zahl jüngster Anforderungen.** Im Protokoll werden nicht mehr als die angegebene Anzahl von Anfragen mit detaillierten Informationen gespeichert. Wenn der Grenzwert erreicht ist, ersetzt jede neue Anforderung mit ausführlichen Informationen die älteste Anforderung im Protokoll.
- **Keine detaillierten Informationen zu irgendeiner Anforderung protokollieren.** Das Änderungsverfolgungsprotokoll enthält nur Basisinformationen zu allen im Protokoll gespeicherten Anforderungen.

Replikation von Verwaltungsverlaufsdaten

Standardmäßig werden die Verwaltungsverlaufsdaten in den Quest One ActiveRoles-Konfigurationsdatenbanken gespeichert. Wenn die Quest One ActiveRoles-Replikation also, wie im Abschnitt „Konfigurieren von Replikationen" weiter unten in diesem Dokument beschrieben, konfiguriert ist, werden die Verwaltungsverlaufdaten gemeinsam mit den anderen Konfigurationsdaten zwischen Verwaltungsdiensten repliziert. Bei einem hohen Verwaltungsverlaufs-Datenvolumen kann dies zu einer beträchtlichen Belastung des Netzwerks führen.

Quest One ActiveRoles gibt Ihnen die Möglichkeit, die Replikation von Verwaltungsverlaufsdaten zu deaktivieren, um die Belastung des Netzwerks zu verringern. Beachten Sie jedoch, dass dies dazu führt, dass jeder Datenbankserver einen eigenen Verwaltungsverlaufsdatenspeicher führt. Dies hat zur Folge, dass Sie den Verwaltungsverlauf verwenden können, um die Änderungen zu untersuchen, die nur über die Verwaltungsdienste vorgenommen wurden, die dieselbe Datenbank wie der Verwaltungsdienst, mit dem Sie verbunden sind, nutzen.

Die Deaktivierung der Replikation von Verwaltungsverlaufsdaten hat folgende Konsequenzen:

- Die durch den Befehl **Verlauf ändern** oder **Benutzeraktivität** generierten Informationen enthalten nur Informationen über die Änderungen, die mit Hilfe einer bestimmten Gruppe von Verwaltungsdiensten durchgeführt wurden (die Dienste, die eine gemeinsame Datenbank nutzen).

  Da die Quest One ActiveRoles-Konsole oder das Web-Interface automatisch den Dienst auswählen, zu dem eine Verbindung hergestellt wird, erhalten Sie während der verschiedenen Verbindungssitzungen möglicherweise verschiedene Berichte für dasselbe Zielobjekt oder Benutzerkonto.

- Die Funktionen von Quest One ActiveRoles, wie etwa der Genehmigungs-Arbeitsablauf, temporäre Gruppenmitgliedschaften und Deprovisionierung aufheben, funktionieren möglicherweise nicht wie erwartet. Einige Vorgänge, die auf diesen Funktionen beruhen, können von Client-Schnittstellen, die mit anderen Verwaltungsdienste verbunden sind, nicht richtig verarbeitet oder angezeigt werden.

  Quest One ActiveRoles verwendet den Verwaltungsverlaufsspeicher zur Speicherung von Genehmigungs- und Deprovisionsaufgaben sowie Aufgaben im Zusammenhang mit temporären Gruppenmitgliedschaften. Ohne Synchronisation der Informationen zwischen Verwaltungsverlaufsspeichern ist eine solche, von einem der Verwaltungsdienste erstellte Aufgabe möglicherweise nicht für andere Verwaltungsdienste verfügbar. Als Folge variiert das Verhalten der Quest One ActiveRoles-Konsole oder des Web-Interface abhängig vom gewählten Verwaltungsdienst.

Die Deaktivierung der Replikation der Verwaltungsverlaufsdaten hat keinen Einfluss auf die Replikation der anderen, mit der Konfiguration von Quest One ActiveRoles verbundenen Daten. Nur der Verwaltungsverlauf-relevante Teil der Konfigurationsdatenbank wird von der Quest One ActiveRoles-Replikation ausgeschlossen.

Die Anweisungen bezüglich der Deaktivierung der Replikation von Verwaltungsverlaufsdaten hängen davon ab, ob die Quest One ActiveRoles-Replikation bereits konfiguriert ist oder nicht.

Replikation noch nicht konfiguriert

Wenn Sie die Quest One ActiveRoles-Replikation erstmalig konfigurieren, können Sie sicherstellen, dass die Verwaltungsverlaufsdaten nicht bei der Quest One ActiveRoles-Replikation berücksichtigt werden, indem Sie die Rolle des „Herausgebers" wie folgt festlegen (eine Definition der Replikationsrollen finden Sie unter „Konfigurieren von Replikationen" weiter unten in diesem Dokument):

1. Stellen Sie über die Quest One ActiveRoles-Konsole eine Verbindung zu dem Verwaltungsdienst her, dessen SQL Server die Rolle als Herausgeber übernehmen soll.
2. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Server Configuration** und wählen Sie den Container **Configuration Databases**.
3. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf die Datenbank und klicken Sie dann auf **Heraufstufen**.
4. Warten Sie, bis die Konsole den Vorgang „Heraufstufen" ausführt.
5. Wählen Sie in der Konsolenstruktur unter **Server Configuration** den Container **Management History Databases**.
6. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf die Datenbank und klicken Sie dann auf **Herabstufen**.
7. Warten Sie, bis die Konsole den Vorgang „Herabstufen" abgeschlossen hat.

Dann können Sie die Quest One ActiveRoles-Replikation mittels der Quest One ActiveRoles-Konsole, wie im Abschnitt „Konfigurieren von Replikationen" weiter unten in diesem Dokument beschrieben, konfigurieren: Verwenden Sie den Befehl **Hinzufügen Replikationspartner** für die Datenbank im Container **Configuration Databases**, um Abonnenten zu dem von Ihnen konfigurierten Herausgeber hinzuzufügen.

Replikation bereits konfiguriert

Dieser Abschnitt enthält Anweisungen bezüglich der Deaktivierung der Replikation von Verwaltungsverlaufsdaten für den Fall, dass die Quest One ActiveRoles-Replikation bereits, wie im Abschnitt „Konfigurieren von Replikationen" weiter unten in diesem Dokument beschrieben, konfiguriert ist. Sie müssen zunächst alle Abonnenten der Verwaltungsverlaufsdaten löschen und dann den Herausgeber für die Verwaltungsverlaufsdaten herabstufen. Hierdurch wird nur die Replikation der Verwaltungsverlaufsdaten gestoppt; die anderen Replikationsfunktionen bleiben erhalten.

Deaktivieren der Replikation von Verwaltungsverlaufsdaten:

1. Stellen Sie über die Quest One ActiveRoles-Konsole eine Verbindung zu dem Verwaltungsdienst her, dessen SQL Server die Rolle des Herausgebers inne hat.
2. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Server Configuration** und wählen Sie den Container **Management History Databases** aus.
3. Verwenden Sie den Befehl **Löschen** für jede der Abonnenten-Datenbanken, um alle Abonnenten im Container **Management History Databases** zu löschen.
4. Klicken Sie mit der rechten Maustaste auf die Herausgeber-Datenbank und klicken Sie dann auf **Herabstufen**.
5. Warten Sie, bis die Konsole den Vorgang „Herabstufen" abgeschlossen hat.

Neukonfiguration der Replikation von Verwaltungsverlaufsdaten

Wenn die Replikation von Verwaltungsverlaufsdaten deaktiviert ist, ist es immer noch möglich, dass mehrere Verwaltungsdienste dasselbe Änderungsverlaufsprotokoll verwenden, indem Sie sie so konfigurieren, dass sie dieselbe Datenbank nutzen. Beachten Sie, dass die Verwaltungsdienst-Version 6.x Ihnen ermöglicht, mehrere Dienste mit der Option, eine einzige Konfigurationsdatenbank zu nutzen, zu installieren. So können Sie den ersten Dienst in Ihrer Umgebung installieren und das Setup-Programm eine Datenbank erstellen lassen. Dann können Sie einen weiteren Dienst installieren, wobei das Setup-Programm den neuen Dienst so konfiguriert, dass dieser dieselbe Datenbank wie der vorhandene Dienst nutzt.

Wenn jedoch verschiedene Verwaltungsdienste in Ihrer Umgebung unterschiedliche Datenbankserver nutzen, müssen Sie die Replikation der Verwaltungsverlaufsdaten möglicherweise neu konfigurieren, um die Verwaltungsverlaufsfunktion mit all ihren Vorteilen nutzen zu können. Verwalten Sie zu diesem Zweck die Objekte im Container **Management History Databases** wie folgt:

Gehen Sie folgendermaßen vor, um die Replikation von Verwaltungsverlaufsdaten neu zu konfigurieren:

1. Stellen Sie über die Quest One ActiveRoles-Konsole eine Verbindung zu dem Verwaltungsdienst her, dessen SQL Server die Rolle des Herausgebers inne hat.
2. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Server Configuration** und wählen Sie den Container **Management History Databases** aus.
3. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf die Datenbank und klicken Sie dann auf **Heraufstufen**.
4. Warten Sie, bis die Konsole den Vorgang „Heraufstufen" ausführt.
5. Verwenden Sie den Befehl **Replikationspartner hinzufügen** für die Herausgeber-Datenbank im Container **Management History Databases**, um Abonnenten für die Verwaltungsverlaufsdaten hinzuzufügen.

Der Befehl **Replikationspartner hinzufügen** startet den Assistenten, der nahezu identisch mit dem im Abschnitt „Hinzufügen von Mitgliedern zu einer Replikationsgruppe" weiter unten in diesem Dokument beschriebenen Assistenten ist. Der einzige Unterschied besteht darin, dass die Liste der Verwaltungsdienste, deren Datenbankserver als Abonnenten für die Verwaltungsverlaufsdaten angegeben werden können, auf die Dienste beschränkt ist, die dieselben, auf dem von Ihnen ausgewählten Herausgeber gehosteten Konfigurationsdaten nutzen.

Zentralisierte Verwaltungsverlaufsspeicherung

Bei Auswahl der Standard-Replikationseinstellungen in Quest One ActiveRoles werden die Verwaltungsverlaufsdaten zusammen mit den Konfigurationsdaten zwischen Replikationspartnern synchronisiert. Bei einem großen Volumen an Verwaltungsverlaufsdaten kann dieses Verhalten zu einer hohen Belastung des Netzwerks führen, was bei bestimmten Szenarien wie etwa beim Hinzufügen eines neuen Partners zur Quest One ActiveRoles-Replikationsgruppe Leistungseinbußen von Quest One ActiveRoles zur Folge haben kann. Hier finden Sie Anweisungen bezüglich der Vermeidung der Replikation von Verwaltungsverlaufsdaten durch die Implementierung einer gemeinsamen Speicherung dieser Daten für alle Replikationspartner.

Die Synchronisation der Verwaltungsverlaufsdaten kann vom Quest One ActiveRoles-Replikationsvorgang entfernt werden, indem Sie eine gemeinsame Speicherung dieser Daten für alle Replikationspartner implementieren. Die gemeinsame Speicherung gewährleistet die Konsolidierung der Teile der Verwaltungsverlaufsdaten, die von verschiedenen Verwaltungsdiensten generiert wurden, während sie gleichzeitig die Notwendigkeit einer Synchronisation dieser Daten zwischen mehreren Speichern vermeidet.

Quest One ActiveRoles bietet die folgenden Optionen, um einen zentralisierten, gemeinsamen Speicher für die Verwaltungsverlaufsdaten zu implementieren:

- Konfigurieren Sie die Verwaltungsdienste so, dass die Konfigurationsdatenbank eines dieser Dienste von den anderen Diensten als Verwaltungsverlaufsspeicher verwendet wird. Auf diese Weise verwenden alle Verwaltungsdienste, die eine gemeinsame Konfiguration nutzen, denselben Verwaltungsverlaufsspeicher – nämlich die Konfigurationsdatenbank, die Sie für diese Rolle auswählen.
- Erstellen Sie eine separate Datenbank, in der die Verwaltungsverlaufsdaten gespeichert werden sollen, und konfigurieren Sie dann die Verwaltungsdienste so, dass sie diese Datenbank anstelle Ihrer Konfigurationsdatenbank als den Verwaltungsverlaufsspeicher nutzen. Auf diese Weise verwenden alle Verwaltungsdienste, die eine gemeinsame Konfiguration nutzen, denselben Verwaltungsverlaufsspeicher – nämlich die von Ihnen erstellte Verwaltungsverlaufsdatenbank.

In diesem Abschnitt wird jede dieser beiden Optionen eingehend beschrieben.

Option 1: Dedizierte Konfigurationsdatenbank für die Speicherung der Verwaltungsverlaufsdaten

Standardmäßig speichert der Verwaltungsdienst sowohl seine Konfigurationsdaten als auch seine Verwaltungsverlaufsdaten in derselben Konfigurationsdatenbank. Folglich müssen bei mehreren Konfigurationsdatenbanken die Verwaltungsverlaufsdaten gemeinsam mit den Konfigurationsdaten per Replikation synchronisiert werden, um die Verwaltungsverlaufsdaten zu konsolidieren.

Quest One ActiveRoles bietet die Möglichkeit, die Verwaltungsdienste, die eine gemeinsame Konfiguration nutzen, neu zu konfigurieren, sodass eine einzige Konfigurationsdatenbank für die Speicherung der Verwaltungsverlaufsdaten für alle Verwaltungsdienste genutzt wird. Diese Option verleiht Ihnen die Flexibilität, die Speicherung von Konfigurationsdaten zu verteilen und gleichzeitig die Speicherung von Verwaltungsverlaufsdaten zu zentralisieren. Gehen Sie wie nachfolgend beschrieben vor, um dieses Szenario zu implementieren.

1. Deaktivieren Sie die Replikation von Verwaltungsverlaufsdaten. Sie können dazu die Quest One ActiveRoles-Konsole wie folgt verwenden: Stellen Sie eine Verbindung zu dem Verwaltungsdienst her, dessen Datenbankserver die Rolle des Herausgebers in der Replikationsgruppe inne hat, rufen Sie dann den Container **Configuration/Server Configuration/Management History Databases/** auf, löschen Sie alle Abonnentenobjekte aus diesem Container und führen Sie dann den Befehl **Herabstufen** für das Herausgeberobjekt in diesem Container aus.
2. Entscheiden Sie, welche Konfigurationsdatenbank als der gemeinsame Speicher für die Verwaltungsverlaufsdaten genutzt werden soll. In diesem Abschnitt wird die Datenbank, die Sie auswählen, als die *Verwaltungsverlaufsdatenbank* bezeichnet.
3. Für jeden Verwaltungsdienst, der seine Konfigurationsdaten in einer anderen Datenbank als in der von Ihnen im vorigen Schritt ausgesuchten Datenbank speichert, führen Sie die im Unterabschnitt „Konfigurieren des Verwaltungsdienstes, sodass dieser die neue Verwaltungsverlaufsdatenbank verwendet“ weiter unten in diesem Abschnitt aufgeführten Schritte durch.

Option 2: Separate Konfigurationsdatenbank für die Speicherung der Verwaltungsverlaufsdaten

Quest One ActiveRoles bietet auch die Möglichkeit, die Verwaltungsverlaufsdaten in einer separaten Verwaltungsverlaufsdatenbank zu speichern, anstatt dieselbe Datenbank für die Speicherung der Konfigurationsdaten und der Verwaltungsverlaufsdaten zu verwenden. Bei Auswahl dieser Option können mehrere Verwaltungsdienste so konfiguriert werden, dass sie eine gemeinsame Verwaltungsverlaufsdatenbank auf einem dedizierten SQL Server verwenden.

Wenn eine Gruppe von Verwaltungsdiensten dieselbe Verwaltungsverlaufsdatenbank nutzen soll, müssen Sie gewährleisten, dass die Verwaltungsdienste in der Gruppe über dieselbe Konfiguration verfügen. Dies kann auf eine der folgenden Weisen erfolgen:

- Verwenden Sie die Quest One ActiveRoles-Replikationsfunktion, um die Konfigurationsdatenbanken zu synchronisieren, die von den Verwaltungsdiensten verwendet werden.
- Achten Sie darauf, dass alle Verwaltungsdienste in der Gruppe dieselbe Konfigurationsdatenbank nutzen.

Mit derselben Konfiguration für alle Verwaltungsdienste einschließlich der Konfiguration des Web-Interface und der verwalteten Domänen vermeiden Sie jegliche Inkonsistenzen in den Verwaltungsverlaufsdaten, die von den Verwaltungsdiensten gemeinsam genutzt werden.

Gehen Sie wie nachfolgend beschrieben vor, um das auf dieser Option beruhende Szenario zu implementieren.

1. Deaktivieren Sie die Replikation von Verwaltungsverlaufsdaten. Sie können dazu die Quest One ActiveRoles-Konsole wie folgt verwenden: Stellen Sie eine Verbindung zu dem Verwaltungsdienst her, dessen Datenbankserver die Rolle des Herausgebers in der Replikationsgruppe inne hat, rufen Sie dann den Container **Configuration/Server Configuration/Management History Databases/** auf, löschen Sie alle Abonnentenobjekte aus diesem Container und führen Sie dann den Befehl **Herabstufen** für das Herausgeberobjekt in diesem Container aus.
2. Erstellen Sie die Verwaltungsverlaufsdatenbank. Anweisungen hierzu finden Sie unter „Erstellen einer Verwaltungsverlaufsdatenbank" weiter unten in diesem Abschnitt.
3. Füllen Sie die neue Verwaltungsverlaufsdatenbank optional mit den Verwaltungsverlaufsdaten, die bereits in Ihrer Quest One ActiveRoles-Umgebung vorhanden sind. Anweisungen hierzu finden Sie unter „Importieren von Daten in die neue Verwaltungsverlaufsdatenbank" weiter unten in diesem Abschnitt.
4. Führen Sie für jeden Verwaltungsdienst die Schritte durch, die im Unterabschnitt „Konfigurieren des Verwaltungsdienstes, sodass dieser die neue Verwaltungsverlaufsdatenbank verwendet" weiter unten in diesem Abschnitt aufgeführt sind.

Erstellen einer Verwaltungsverlaufsdatenbank

Um eine Verwaltungsverlaufsdatenbank zu erstellen, verwenden Sie die SQL-Skripts, die sich im Ordner **Verschiedenes\MH-Datenbank erstellen** auf der Quest One ActiveRoles-DVD befinden. Führen Sie auf dem Computer, auf dem SQL Server installiert ist, die Datei CreateDB.bat aus und führen Sie dann die Datei Create_MHOnly.bat aus. Jede dieser Dateien weist die folgenden Parameter auf:

- Erster Parameter (erforderlich). Gibt die SQL Server-Instanz in der Form *Computername* für eine Standardinstanz oder *Computername**Instanzname* für eine benannte Instanz an, auf der Sie die Datenbank erstellen möchten.
- Zweiter Parameter (erforderlich). Name der Datenbank, die Sie erstellen möchten.

- Dritter Parameter (optional). SQL Server-Login, mit dem Sie sich bei SQL Server anmelden möchten (impliziert die SQL Server-Authentifizierung). Wenn der dritte Parameter nicht angegeben wird, verwendet das Skript die Windows-Authentifizierung mit den Anmeldeinformationen des aktuell angemeldeten Benutzers.
- Vierter Parameter (optional). Passwort des SQL Server-Logins. Geben Sie diesen Parameter nicht an, wenn das Login über ein leeres Kennwort verfügt.

Beispiel: Die folgende Befehlssequenz Erstellen der Datenbank mit dem Namen „ChangeHistory" in der Instanz „MyServer\ARS" von SQL Server, wobei der Vorgang im Sicherheitskontext des aktuell angemeldeten Benutzers durchgeführt wird:

```
CreateDB.bat "MyServer\ARS " "[ChangeHistory]"
Create_MHOnly.bat "MyServer\ARS " "ChangeHistory"
```

Um die Datenbank zu erstellen, geben Sie den ersten Befehl in der Eingabeaufforderung ein und warten Sie, während das Skript den Vorgang ausführt. Wenn der Vorgang CreateDB abgeschlossen ist, geben Sie den zweiten Befehl ein.

Importieren von Daten in die neue Verwaltungsverlaufsdatenbank

Sie müssen möglicherweise die neu erstellte Verwaltungsverlaufsdatenbank mit ihren vorhandenen Verwaltungsverlaufsdaten füllen, sodass die Daten für die Quest One ActiveRoles-Benutzerschnittstellen verfügbar bleiben, nachdem Sie den Verwaltungsdienst für die Verwendung des neuen Verwaltungsverlaufsspeichers konfiguriert haben. Verwenden Sie hierzu den Verwaltungsverlauf-Migrations-Assistenten, der Teil der Quest One ActiveRoles-Verwaltungsdienstinstallation ist.

Der Assistent führt die in den Quelldatenbanken gefundenen Verwaltungsverlaufsdaten, wie etwa die Quest One ActiveRoles-Konfigurationsdatenbank, mit den in der Verwaltungsverlaufsdatenbank gespeicherten Daten zusammen. Beachten Sie, dass der Assistent nur neue Daten hinzufügt und jegliche bereits in der Verwaltungsverlaufsdatenbank enthaltene Daten erhalten bleiben. Sie können die alten Verwaltungsverlaufsdaten jederzeit importieren, nachdem Sie den Verwaltungsdienst auf den neuen Verwaltungsverlaufsspeicher umgeleitet haben, ohne einen Datenverlust fürchten zu müssen.

Der Assistent fragt Sie zunächst nach der Datenbank, aus der Daten importiert werden sollen. Sie können Daten aus der Konfigurationsdatenbank importieren, die vom Verwaltungsdienst verwendet wird. Als nächstes fragt Sie der Assistent nach der Datenbank, in die Sie die Daten importiert möchten. Geben Sie die von Ihnen erstellte Verwaltungsverlaufsdatenbank an. Dann fragt Sie der Assistent, ob Sie alle Datensätze oder nur einen bestimmten Datensatzbereich importieren möchten. Sie können sich entscheiden, nicht alle Datensätze zu importieren, da der Import großer Datenmengen mehrere Stunden in Anspruch nehmen kann. Abschließend überträgt der Assistent die Daten. Ausführliche Anweisungen über die Verwendung des Assistenten finden Sie im Abschnitt „Importieren von Verwaltungsverlaufsdaten" im *Quest One ActiveRoles – Erste Schritte*.

Konfigurieren des Verwaltungsdienstes, sodass dieser die neue Verwaltungsverlaufsdatenbank verwendet

Gehen Sie wie nachfolgend beschrieben vor, um den Verwaltungsdienst auf den neuen Verwaltungsverlaufsspeicher umzuleiten.

1. Stoppen Sie den Verwaltungsdienst. Geben Sie hierzu den folgenden Befehl an der Eingabeaufforderung des Computers ein, auf dem der Verwaltungsdienst ausgeführt wird: **net stop arssvc**
2. Konfigurieren Sie die neuen Verbindungseinstellungen. Wechseln Sie an der Eingabeaufforderung zu dem Quest One ActiveRoles-Installationsverzeichnis (standardmäßig ist dies C:\Programme\Quest Software\Quest One ActiveRoles\), geben Sie einen Befehl auf der Grundlage der folgenden Syntax ein und führen Sie dann den Befehl aus.

   Befehlssyntax:

   ```
   arssvc.exe /dbMHServerName <instance> /dbMHName <name> /
   dbMHAuthenticationMode <0 | 1> /dbMHLogin <login> /dbMHPassword <password>
   ```

   Ersetzen Sie in dieser Syntax die Platzhalter durch die tatsächlichen Parameterwerte:

   - Ersetzen Sie in /dbMHServerName <instance> den Wert <instance> durch die Zeichenkette, die die SQL Server-Instanz angibt, die die neue Verwaltungsverlaufsdatenbank hostet. Geben Sie diese Zeichenkette in der Form *Computername* für eine Standardinstanz oder *Computername**Instanzname* für eine benannte Instanz an.
   - Ersetzen Sie in /dbMHName <name> den Wert <name> durch den Namen der Verwaltungsverlaufsdatenbank.
   - Geben Sie in /dbMHAuthenticationMode <0 | 1> entweder 0 oder 1 anstelle von <0 | 1> ein, um den Authentifizierungsmodus der Verwaltungsdienstverbindung mit der Verwaltungsverlaufsdatenbank festzulegen:
   - /dbMHAuthenticationMode 0 führt dazu, dass der Verwaltungsdienst die SQL Server-Authentifizierung verwendet (diese Einstellung erfordert, dass Sie auch die Parameter /dbMHLogin und /dbMHPassword angeben; der Verwaltungsdienst verwendet das angegebene Login und Kennwort für den Verbindungsaufbau zur Datenbank)
   - /dbMHAuthenticationMode 1 führt dazu, dass der Verwaltungsdienst die Windows-Authentifizierung verwendet (bei Auswahl von dieser Einstellung haben die Parameter /dbMHLogin und /dbMHPassword keinen Einfluss; der Verwaltungsdienst verwendet sein Dienstkonto für den Verbindungsaufbau zur Datenbank)
   - Ersetzen Sie in /dbMHLogin <login> den Wert <login> durch den Namen des SQLServer-Login, der für die SQL Server-Authentifizierung verwendet werden soll (dieser Parameter hat nur dann Auswirkungen, wenn /dbMHAuthenticationMode auf 0 gesetzt ist).
   - Ersetzen Sie in /dbMHPassword <password> den Wert <password> durch das Kennwort des SQL Server-Login (dieser Parameter hat nur dann Auswirkungen, wenn /dbMHAuthenticationMode auf 0 gesetzt ist).

   Beispiel: Der folgende Befehl konfiguriert den Verwaltungsdienst so, dass er Verwaltungsverlaufsdaten in der Datenbank „ChangeHistory" in der MyServer\ARS0 von SQL Server speichert, wobei der verwendete Authentifizierungsmodus auf Windows-Authentifizierung gesetzt ist:

   ```
   arssvc.exe /dbMHServerName "MyServer\ARS " /dbMHName "ChangeHistory" /
   dbMHAuthenticationMode 1
   ```

3. Aktualisieren Sie die Konfigurationsdatenbank, um einen Verweis auf die neue Verwaltungsverlaufsdatenbank für den Verwaltungsdienst zu erstellen. Verwenden Sie die folgende Syntax, um ein SQL-Skript zu erstellen, und führen Sie das SQL-Skript auf dem SQL Server aus, der die Konfigurationsdatenbank hostet, wobei Sie die Konfigurationsdatenbank als das Ziel auswählen:

   ```
   update ARServices set edsaMHSQLAlias = '<instance>', edsaMHDatabaseName =
   '<name>' where edsaEdmServiceComputerName = '<ARSServiceName>'
   ```

   Ersetzen Sie in dieser Syntax die Platzhalter durch die tatsächlichen Werte:

   - Ersetzen Sie <instance> durch die Zeichenkette, die die SQL Server-Instanz angibt, die die neue Verwaltungsverlaufsdatenbank hostet. Geben Sie diese Zeichenkette in der Form *Computername* für eine Standardinstanz oder *Computername**Instanzname* für eine benannte Instanz an. Dies ist die von Ihnen in Schritt 2 angegebene SQL Server-Instanz.
   - Ersetzen Sie <name> durch den Namen der Verwaltungsverlaufsdatenbank. Dies ist der von Ihnen in Schritt 2 angegebene Datenbankname.
   - Ersetzen Sie <ARSServiceName> durch den vollqualifizierten DNS-Namen des Computers, auf dem der Verwaltungsdienst installiert ist.

   Beispiel: Vorausgesetzt, dass die SQL Server-Instanz und der Datenbankname identisch mit den Angaben im Beispiel in Schritt 2 sind und vorausgesetzt, dass der Name des Verwaltungsdienstcomputers „ARSService.mycompany.com" ist, lautet das SQL-Skript wie folgt:

   ```
   update ARServices set edsaMHSQLAlias = 'MyServer\ARS ', edsaMHDatabaseName =
   'ChangeHistory' where edsaEdmServiceComputerName = 'ARSService.mycompany.com'
   ```

4. Starten Sie den Verwaltungsdienst. Geben Sie hierzu den folgenden Befehl an der Eingabeaufforderung des Computers ein, auf dem der Verwaltungsdienst installiert ist: **net start arssvc**

Wichtig. In einer Umgebung, in der mehrere Verwaltungsdienstinstanzen gemeinsam eine einzige Konfigurationsdatenbank nutzen, muss das oben aufgeführte Verfahren wie folgt durchgeführt werden:

1. Stoppen Sie alle Verwaltungsdienstinstanzen, die die betreffende Konfigurationsdatenbank nutzen.
2. Konfigurieren Sie für jede dieser Verwaltungsdienstinstanzen die Verbindungseinstellungen wie in Schritt 2 beschrieben und führen Sie das Skript in Schritt 3 aus, wobei Sie <ARSServiceName> durch den DNS-Namen des entsprechenden Verwaltungsdienstcomputers ersetzen.
3. Nachdem Schritt 2 und Schritt 3 für alle Verwaltungsdienstinstanzen abgeschlossen sind, starten Sie jede der Verwaltungsdienstinstanzen.

Untersuchen des Änderungsverlaufs

Auf das Änderungsverlaufsprotokoll können Sie von der Quest One ActiveRoles-Konsole aus zugreifen. So können Sie schnell untersuchen, welche Änderungen an einem bestimmten Benutzer oder einer bestimmten Gruppen vorgenommen wurden und wer diese wann vorgenommen hat. Wenn beispielsweise ein Kennwort mit Hilfe von Quest One ActiveRoles zurückgesetzt wurde, können Sie im Änderungsverlauf anzeigen, wer dies getan hat und wann.

Um Änderungen an einem bestimmten Objekt (z. B. an einem Benutzer- oder Gruppenobjekt) zu untersuchen, klicken Sie auf der Quest One ActiveRoles-Konsole mit der rechten Maustaste auf das Objekt und klicken Sie dann auf **Änderungsverlauf**.

Standardmäßig werden im Fenster **Änderungsverlauf** nur grundlegende Optionen angezeigt. Sie können weitere Optionen anzeigen, indem Sie auf das Plus-Zeichen (+) in der oberen linken Ecke neben der ersten Spaltenüberschrift klicken.

Im Fenster **Änderungsverlauf** finden Sie die folgenden Informationen:

- **Name.** Der Name des Objekts, für das Sie den Änderungsverlauf untersuchen.
- **Angefordert.** Datum und Uhrzeit der angeforderten Änderungen.
- **Angefordert von.** Das Benutzerkonto, das die Änderungen angefordert hat.
- **Abgeschlossen.** Datum und Uhrzeit der übernommenen Änderungen.
- **Eigenschaften.** Die Eigenschaften des geänderten Objekts, einschließlich Informationen über die geänderten Eigenschaftswerte.
- **Status.** Gibt an, ob die angeforderten Änderungen übernommen wurden (Status ABGESCHLOSSEN) oder die Genehmigung abgewartet wird (Status AUSSTEHEND).

Das Fenster **Änderungsverlauf** umfasst auch die folgenden Bereiche:

- **Während dieses Vorgangs geänderte Eigenschaften.** Informationen über die Objekteigenschaftswerte, die geändert wurden (alte Werte), über die den Eigenschaften zugeordnete neue Werte und über das Benutzerkonto, das für die Durchführung der Änderungen verwendet wurde.
- **Arbeitsablaufaktivitäten und Richtlinienaktionen.** Detaillierte Informationen über alle Richtlinien und Arbeitsabläufe, die Quest One ActiveRoles bei der Verarbeitung der Änderungsanforderung durchgeführt hat.
- **Vorgangsdetails.** Zusätzliche Informationen darüber, wann und von wem die Änderungen angefordert wurden.

Im Bereich **Arbeitsablaufaktivitäten und Richtlinienaktionen** wird ein Bericht der Richtlinienaktionen und Aktionen der Arbeitsablaufaktivität angezeigt. Der Bericht organisiert die Aktionsergebnisse in Bereiche, wobei jeder Bereich für eine einzelne Richtlinie oder Aktivität spezifische Berichtselemente enthält. Sie können den Bereich erweitern, indem Sie auf den Titel klicken. Um einen Abschnitt zu erweitern, klicken Sie auf den Titel des Abschnittes. Für bestimmte Elemente steht im Bericht die Option zur Verfügung, die Ansicht weiter zu erweitern und zusätzliche Informationen anzuzeigen. Durch Anklicken der Option **Liste** wird eine Liste von Elementen (z. B. Benutzer- oder Gruppeneigenschaften) angezeigt, die von der Richtlinie oder Aktivität betroffen sind. Indem Sie auf die Option **Details** klicken, können Sie die Richtlinie oder das Ergebnis des Aktivitätsvorgangs detaillierter untersuchen.

In den folgenden Themen sind die Abschnitte und Berichtselemente aufgeführt, die im Bereich **Arbeitsablaufaktivitäten und Richtlinienaktionen** angezeigt werden können. Jeder Abschnitt im Bericht beschreibt die Ergebnisse der von einer Arbeitsablaufaktivität oder Richtlinie durchgeführten Aktion. Die Berichtselemente innerhalb des Abschnitts informieren über den Erfolg oder das Fehlschlagen der Aktion der Richtlinie oder Aktivität. Bei einem Fehler enthält das Berichtselement eine Fehlerbeschreibung.

Nicht alle aufgelisteten Abschnitte und Elemente müssen notwendigerweise in einem Bericht enthalten sein. Ein aktueller Bericht umfasst nur Abschnitte, die den Arbeitsablaufaktivitäten und Richtlinien entsprechen, die ActiveRoles bei der Verarbeitung der Vorgangsanforderung ausführt.

Die folgenden Themen gehen näher auf die Berichtsabschnitte und -elemente ein, die im Bereich **Arbeitsablaufaktivitäten und Richtlinienaktionen** angezeigt werden:

- Arbeitsablaufaktivität – Berichtsabschnitte
- Berichtselemente der Richtlinie
- Berichtselemente der internen Richtlinie von ActiveRoles

Arbeitsablaufaktivität – Berichtsabschnitte

In einem Änderungsverlaufsbericht sind in den für Arbeitsablaufaktivitäten spezifischen Berichtsabschnitten alle Aktivitäten aufgeführt, die ActiveRoles während der Verarbeitung einer bestimmten Vorgangsanforderung ausgeführt hat. Für jede Aktivität können Sie ausgehend vom entsprechenden Berichtsabschnitt festlegen, ob die Aktivität erfolgreich abgeschlossen wurde oder Fehler ausgegeben wurden. Bei einem Fehler enthält der Berichtsabschnitt eine Fehlerbeschreibung. Bei Aktivitäten, die Änderungen an Verzeichnisdaten erfordern (z.B. Aktivitäten, die neue Objekte erstellen oder vorhandene Objekte ändern), können Sie die angeforderten Änderungen im Detail überprüfen, indem Sie auf die Vorgangs-ID-Nummer im Berichtsabschnitt anklicken.

In diesem Thema werden die Inhalte der Aktivitätsberichtsabschnitte aufgeführt, die in einem Änderungsverlaufsbericht angezeigt werden können. Jeder Berichtsabschnitt hat eine Kopfzeile, die den Namen der Aktivität, das Zielobjekt der Aktivität (das Objekt wie etwa einen Benutzer, eine Gruppe oder einen Computer, auf den die Aktivität angewandt wird oder wirkt), den Zeitpunkt, zu dem die Aktivität ausgeführt wurde, und den Namen des Arbeitsablaufs, der die Aktivität enthält, angibt. Falls die Aktivität einen Fehler erkannt hat, dann wird der Text in der Kopfzeile des Aktivitätsberichtabschnitts rot angezeigt. Sie können den Berichtsabschnitt erweitern, indem Sie auf die Kopfzeile klicken, um den Text des Berichtabschnitts anzuzeigen. Der Inhalt des Hauptteils variiert abhängig vom Aktivitätstyp. Bei einer Fehlerbedingung zeigt der Hauptteil eine Fehlerbeschreibung an.

Des Weiteren deckt dieses Thema die Inhalte des Textes des Berichtsabschnittes für jeden Aktivitätstyp in Situationen ab, in denen keine Fehler aufgetreten sind.

Aktivität „Genehmigung"

Der spezifische Berichtsabschnitt einer Genehmigungsaktivität enthält Informationen über die Genehmigungsaufgabe, die von dieser Aktivität erstellt wurde, und variiert je nach Status der Genehmigungsaufgabe. Normalerweise erstellt die Aktivität keine Genehmigungsaufgabe, wenn der genehmigungspflichtige Vorgang von einem ActiveRoles-Administrator oder einer genehmigenden Instanz angefordert wird. In diesem Fall zeigt der Text des Abschnittes eine Nachricht an, die darauf hinweist, dass die Aktivität umgangen wird. Andernfalls wird der Text des Berichtsabschnittes folgenden Inhalt haben.

Aufgabenstatus: Ausstehend

Die folgenden Informationen werden angezeigt, wenn die Aufgabe auf eine Aktion der genehmigenden Instanz wartet.

- **Details der Genehmigungsaufgabe**
  - Aufgaben-ID: <Nummer>
  - Anrede: <Bezeichnung der Genehmigungsaufgabe>
  - Status: Ausstehend
  - Angefordert: <Datum und Uhrzeit der Aufgabenerstellung>
  - Angefordert von: <Name,der angibt, wer den Vorgang angefordert hat>

Aufgabenstatus: Abgeschlossen

Die folgende Information wird angezeigt, wenn die genehmigende Instanz den angeforderten Vorgang gestattet.

- **Von der genehmigenden Instanz geänderte Eigenschaften**
  - Eigenschaft <Eigenschaft des Vorgangszielobjekts, die von der genehmigenden Instanz festgelegt oder geändert wurde>
  - Geändert in <Eigenschaftswert, der von der genehmigenden Instanz geliefert wurde>
- **Details der Genehmigungsaufgabe**
  - Aufgaben-ID: <Nummer>
  - Anrede: <Bezeichnung der Genehmigungsaufgabe>
  - Status: Abgeschlossen
  - Angefordert: <Datum und Uhrzeit der Aufgabenerstellung>
  - Angefordert von: <Name,der angibt, wer den Vorgang angefordert hat>
  - Abgeschlossen: <Datum und Uhrzeit des Aufgabenabschlusses>
  - Abgeschlossen von: <Name der genehmigenden Instanz, die die Aufgabe ausgeführt hat>
  - Grund für den Abschluss: <Von der genehmigenden Instanz gelieferter Text>
  - Aktion der genehmigenden Instanz: <Entscheidung, die die genehmigende Instanz trifft, um den Vorgang zu gestatten>

Aufgabenstatus: Abgelehnt

Die folgende Information wird angezeigt, wenn die genehmigende Instanz den angeforderten Vorgang ablehnt.

- **Details der Genehmigungsaufgabe**
  - Aufgaben-ID: <Nummer>
  - Anrede: <Bezeichnung der Genehmigungsaufgabe>
  - Status: Abgelehnt
  - Angefordert: <Datum und Uhrzeit der Aufgabenerstellung>
  - Angefordert von: <Name,der angibt, wer den Vorgang angefordert hat>
  - Abgelehnt: <Datum und Uhrzeit des Aufgabenabschlusses>
  - Abgelehnt von: <Name der genehmigenden Instanz, die die Aufgabe ausgeführt hat>
  - Grund für die Ablehnung: <Von der genehmigenden Instanz gelieferter Text>
  - Aktion der genehmigenden Instanz: <Entscheidung, die die genehmigende Instanz trifft, um den Vorgang abzulehnen>

Aufgabenstatus: Abgebrochen

Die folgende Information wird angezeigt, wenn die Genehmigungsaufgabe abgebrochen wurde.

- **Details der Genehmigungsaufgabe**
  - Aufgaben-ID: <Nummer>
  - Anrede: <Bezeichnung der Genehmigungsaufgabe>
  - Status: Abgebrochen
  - Angefordert: <Datum und Uhrzeit der Aufgabenerstellung>
  - Angefordert von: <Name,der angibt, wer den Vorgang angefordert hat>
  - Abgebrochen: <Datum und Uhrzeit des Aufgabenabbruchs>

- Abgebrochen von: <gibt an, wer die Aufgabe abgebrochen hat>
- Grund für den Abbruch: <gibt an, warum die Aufgabe abgebrochen wurde>

Aufgabenstatus: Beliebig

Die folgenden Informationen werden immer zusätzlich zu den Details der Genehmigungsaufgabe angezeigt.

- Einstellungen der Genehmigungsaufgabe:
  - Genehmigende Instanzen: <Liste der Namen, die angeben, wer befugt ist, den Vorgang zu genehmigen>
  - Mögliche Aktionen der genehmigenden Instanz: <Liste der Entscheidungen, die der genehmigenden Instanz zur Auswahl stehen>
  - Die genehmigende Instanz ist aufgefordert, diese Eigenschaften zu liefern oder zu ändern: <Liste der Eigenschaftsnamen>
  - Die genehmigende Instanz darf Änderungen an den zur Genehmigung gesendeten Eigenschaften vornehmen: <Ja | Nein>

„Skript"-Aktivität

Wenn bei der Aktivität keine Fehler festgestellt wurden, zeigt der Text des Berichtsabschnittes die folgende Nachricht an:

- Die Aktivität hat das Skript „*Name*" erfolgreich ausgeführt.

Andernfalls wird eine Nachricht angezeigt, die darauf hinweist, dass bei der Aktivität ein Fehler festgestellt wurde. Sie können eine Fehlerbeschreibung im Text des Berichtsabschnittes anzeigen.

Aktivität „Stoppen/Unterbrechen"

Der Text des Berichtsabschnittes zeigt die von der Aktivität bereitgestellte Benachrichtigungsmeldung an. Sie können bei der Konfiguration einer Stoppen/Unterbrechen-Aktivität eine Benachrichtigungsmeldung festlegen.

Aktivität „Berichtsabschnitt hinzufügen"

Kopf und Text des Berichtsabschnittes zeigen die von der Aktivität bereitgestellten Textinformationen an. Sie können bei der Konfiguration einer Aktivität „Berichtsabschnitt hinzufügen" Kopf und Text des Berichtsabschnittes festlegen.

Aktivität „Erstellen"

Der Text des Berichtsabschnittes identifiziert das von der Aktivität erstellte Objekt (Aktivitätszielobjekt) und stellt die folgenden Informationen bereit:

- Objekttyp (z. B. einen Benutzer, eine Gruppe oder einen Computer)
- Name: <Name des Objekts>
- Vorgangs-ID: <Nummer>
- Angefordert: <Datum und Uhrzeit der Vorgangsanforderung>
- Status: <gibt an, ob der Vorgang abgeschlossen oder ausstehend ist>

Sie können auf die Vorgangs-ID-Nummer klicken, um den Vorgang der Objekterstellung im Detail zu untersuchen. Hierdurch wird ein Änderungsverlaufsbericht angezeigt, der Informationen über alle Arbeitsablaufaktivitäten und Richtlinienaktionen enthält, die ActiveRoles in Verbindung mit diesem

Vorgang ausführt. Inhalt und Aufbau dieses Berichts gleichen dem eines normalen Änderungsverlaufsberichts für das neu erstellte Objekt.

Aktivität „Aktualisieren"

Der Text des Berichtsabschnittes identifiziert das von der Aktivität geänderte Objekt (Aktivitätszielobjekt) und stellt die folgenden Informationen bereit:

- Objekttyp (z. B. einen Benutzer, eine Gruppe oder einen Computer)
- Name: <Name des Objekts>
- Vorgangs-ID: <Nummer>
- Angefordert: <Datum und Uhrzeit der Vorgangsanforderung>
- Liste der durch die Aktivität geänderten Objekteigenschaften
- Für jede Eigenschaft wird der von der Aktivität festgelegte Wert (neuer Wert) und der Wert der Eigenschaft vor Änderung durch die Aktivität (alter Wert) angezeigt
- Status: <gibt an, ob der Vorgang abgeschlossen oder ausstehend ist>

Sie können auf die Vorgangs-ID-Nummer klicken, um den Vorgang der Objektänderung im Detail zu untersuchen. Hierdurch wird ein Änderungsverlaufsbericht angezeigt, der Informationen über alle Arbeitsablaufaktivitäten und Richtlinienaktionen enthält, die ActiveRoles in Verbindung mit diesem Vorgang ausführt. Inhalt und Aufbau dieses Berichts gleichen dem eines normalen Änderungsverlaufsberichts für ein Objekt.

Aktivität „Zu einer Gruppe hinzufügen"

Für jede Gruppe, zu der das Aktivitätszielobjekt durch die Aktivität hinzufügt wird, zeigt der Text des Berichtsabschnittes die folgenden Informationen an:

- Name des Objekts
- Name der Gruppe
- Vorgangs-ID: <Nummer>
- Angefordert: <Datum und Uhrzeit der Vorgangsanforderung>
- Status: <gibt an, ob der Vorgang abgeschlossen oder ausstehend ist>

Sie können auf die Vorgangs-ID-Nummer klicken, um den Vorgang der Objekthinzufügung zur Gruppe im Detail zu untersuchen. Hierdurch wird ein Änderungsverlaufsbericht angezeigt, der Informationen über alle Arbeitsablaufaktivitäten und Richtlinienaktionen enthält, die ActiveRoles in Verbindung mit diesem Vorgang ausführt. Inhalt und Aufbau dieses Berichts gleichen dem eines normalen Änderungsverlaufsberichts in Bezug auf Änderungen der Mitgliederliste einer Gruppe.

Aktivität „Aus einer Gruppe entfernen"

Für jede Gruppe, aus der das Aktivitätszielobjekt durch die Aktivität entfernt wird, zeigt der Text des Berichtsabschnittes die folgenden Informationen an:

- Name des Objekts
- Name der Gruppe
- Vorgangs-ID: <Nummer>
- Angefordert: <Datum und Uhrzeit der Vorgangsanforderung>
- Status: <gibt an, ob der Vorgang abgeschlossen oder ausstehend ist>

Sie können auf die Vorgangs-ID-Nummer klicken, um den Vorgang der Objektentfernung aus der Gruppe im Detail zu untersuchen. Hierdurch wird ein Änderungsverlaufsbericht angezeigt, der Informationen über alle Arbeitsablaufaktivitäten und Richtlinienaktionen enthält, die ActiveRoles in Verbindung mit diesem Vorgang ausführt. Inhalt und Aufbau dieses Berichts gleichen dem eines normalen Änderungsverlaufsberichts in Bezug auf Änderungen der Mitgliederliste einer Gruppe.

Aktivität „Verschieben"

Der Text des Berichtsabschnittes identifiziert das Objekt, das von der Aktivität in einen bestimmten Container verschoben wird (Aktivitätszielobjekt), und stellt die folgenden Informationen bereit:

- Objekttyp (z. B. einen Benutzer, eine Gruppe oder einen Computer)
- Name: <Name des Objekts>
- Verschoben in: <Identifiziert den Zielcontainer für die Verschiebung>
- Vorgangs-ID: <Nummer>
- Angefordert: <Datum und Uhrzeit der Vorgangsanforderung>
- Status: <gibt an, ob der Vorgang abgeschlossen oder ausstehend ist>

Sie können auf die Vorgangs-ID-Nummer klicken, um den Vorgang der Objektverschiebung im Detail zu untersuchen. Hierdurch wird ein Änderungsverlaufsbericht angezeigt, der Informationen über alle Arbeitsablaufaktivitäten und Richtlinienaktionen enthält, die ActiveRoles in Verbindung mit diesem Vorgang ausführt. Inhalt und Aufbau dieses Berichts gleichen dem eines normalen Änderungsverlaufsberichts für ein Objekt, das in einen anderen Container verschoben wurde.

Aktivität „Deprovisionieren"

Der Text des Berichtsabschnittes identifiziert das von der Aktivität deprovisionierte Objekt (Aktivitätszielobjekt) und stellt die folgenden Informationen bereit:

- Objekttyp (z. B. einen Benutzer oder eine Gruppe)
- Name: <Name des Objekts>
- Vorgangs-ID: <Nummer>
- Angefordert: <Datum und Uhrzeit der Vorgangsanforderung>
- Status: <gibt an, ob der Vorgang abgeschlossen oder ausstehend ist>

Sie können auf die Vorgangs-ID-Nummer klicken, um den Vorgang der Objektdeprovisionierung im Detail zu untersuchen. Hierdurch wird ein Änderungsverlaufsbericht angezeigt, der Informationen über alle Arbeitsablaufaktivitäten und Richtlinienaktionen enthält, die ActiveRoles in Verbindung mit diesem Vorgang ausführt. Inhalt und Aufbau dieses Berichts gleichen dem eines normalen Änderungsverlaufsberichts für ein Objekt, das deprovisioniert wurde.

Aktivität „Deprovisionierung aufheben"

Der Text des Berichtsabschnittes identifiziert das Objekt, das von der Aktivität aus dem deprovisionierten Zustand wiederhergestellt wird (Aktivitätszielobjekt), und stellt die folgenden Informationen bereit:

- Objekttyp (z. B. einen Benutzer oder eine Gruppe)
- Name: <Name des Objekts>
- Vorgangs-ID: <Nummer>
- Angefordert: <Datum und Uhrzeit der Vorgangsanforderung>
- Status: <gibt an, ob der Vorgang abgeschlossen oder ausstehend ist>

Sie können auf die Vorgangs-ID-Nummer klicken, um den Vorgang der Wiederherstellung des deprovisionierten Objekts im Detail zu untersuchen. Hierdurch wird ein Änderungsverlaufsbericht angezeigt, der Informationen über alle Arbeitsablaufaktivitäten und Richtlinienaktionen enthält, die ActiveRoles in Verbindung mit diesem Vorgang ausführt. Inhalt und Aufbau dieses Berichts gleichen dem eines normalen Änderungsverlaufsberichts für ein Objekt, das aus dem deprovisionierten Zustand wiederhergestellt wurde.

Aktivität „Löschen"

Der Text des Berichtsabschnittes identifiziert das von der Aktivität gelöschte Objekt (Aktivitätszielobjekt) und stellt die folgenden Informationen bereit:

- Objekttyp (z. B. einen Benutzer oder eine Gruppe)
- Name: <Name des Objekts>
- Vorgangs-ID: <Nummer>
- Angefordert: <Datum und Uhrzeit der Vorgangsanforderung>
- Status: <gibt an, ob der Vorgang abgeschlossen oder ausstehend ist>

Sie können auf die Vorgangs-ID-Nummer klicken, um den Vorgang der Objektlöschung im Detail zu untersuchen. Hierdurch wird ein Änderungsverlaufsbericht angezeigt, der Informationen über alle Arbeitsablaufaktivitäten und Richtlinienaktionen enthält, die ActiveRoles in Verbindung mit diesem Vorgang ausführt.

Berichtselemente der Richtlinie

In diesem Thema werden die Elemente des Änderungsverlaufsberichts aufgeführt, die spezifisch für die Richtlinien sind, die mit Hilfe von Richtlinienobjekten in Quest One ActiveRoles angewandt werden. Bei der Ausführung einer bestimmten Richtlinie fügt ActiveRoles einen Berichtsabschnitt hinzu, der die von dieser Richtlinie durchgeführten Aktionen beschreibt. Der Berichtsabschnitt gibt die Richtlinienkategorie und das Richtlinienobjekt an, das die Richtlinie enthält, und informiert über den Erfolg oder das Fehlschlagen der Richtlinienaktion.

In den folgenden Tabellen sind die möglichen Berichtselemente aufgelistet. Es ist eine Tabelle pro Abschnitt vorhanden. Die Elemente in den einzelnen Abschnitten beschreiben die Ergebnisse der Aktionen, die in Übereinstimmung mit der entsprechenden Richtlinie ausgeführt wurden. Berichtselemente enthalten außerdem Informationen zum Erfolg oder Fehler jeder Richtlinienaktion. Bei einem Fehler enthält das Berichtselement eine Fehlerbeschreibung.

Nicht alle aufgelisteten Elemente müssen notwendigerweise in einem Bericht enthalten sein. Ein aktueller Bericht umfasst nur Berichtselemente, die den Richtlinien entsprechen, die ActiveRoles bei der Verarbeitung der Vorgangsanforderung ausführt.

Dieses Thema deckt die Bereitstellungsrichtlinien von ActiveRoles ab. Die spezifischen Berichtsabschnitte für Deprovisionierungsrichtlinien sind in den Themen „Bericht zu Ergebnissen der Deprovision" und „Bericht über die Ergebnisse der Aufhebung der Deprovisionierung" weiter oben in diesem Dokument aufgeführt.

Berichtsabschnitt: Richtlinie „Erzeugung von Benutzeranmeldenamen" wird ausgeführt

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Der Benutzeranmeldename (Prä-Windows 2000) ist auf '*Wert*' gesetzt.	*Nicht zutreffend*

Berichtsabschnitt: Richtlinie „E-Mail-Aliaserzeugung" wird ausgeführt

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Der E-Mail-Alias wird auf '*Alias*' gesetzt.	*Nicht zutreffend*
• Die Eigenschaft 'Alias (mailNickName)' wird aus der Vorgangsanforderung entfernt, weil keine Exchange-Aufgaben angefordert wurden.	*Nicht zutreffend*

Berichtsabschnitt: Richtlinie „Automatische Bereitstellung des Exchange-Postfachs" wird ausgeführt

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Die Postfachdatenbank wird auf '*Datenbankname*' gesetzt.	*Nicht zutreffend*
• Die Option zur Erstellung des Postfachs ist standardmäßig aktiviert.	*Nicht zutreffend*
• Die Option zur Erstellung des Postfachs ist standardmäßig nicht aktiviert.	*Nicht zutreffend*
• Die Änderung der Option zur Erstellung des Postfachs ist zulässig.	*Nicht zutreffend*
• Die Änderung der Option zur Erstellung des Postfachs ist unzulässig.	*Nicht zutreffend*

Berichtsabschnitt: Richtlinie „Automatische Bereitstellung der Gruppenmitgliedschaft" wird ausgeführt

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Das Objekt wird zu den folgenden Gruppen hinzugefügt. Liste: *Gruppennamen*	• Das Objekt kann nicht zu den folgenden Gruppen hinzugefügt werden. Liste: *Gruppennamen und Fehlerbeschreibung*
• Das Objekt wird nicht zu den folgenden Gruppen hinzugefügt, weil es bereits Mitglied dieser Gruppen ist. Liste: *Gruppennamen*	*Nicht zutreffend*
• Das Objekt wird aus den folgenden Gruppen entfernt. Liste: *Gruppennamen*	• Das Objekt kann nicht aus den folgenden Gruppen entfernt werden. Liste: *Gruppennamen und Fehlerbeschreibung*
• Das Objekt wird nicht aus den folgenden Gruppen entfernt, weil es kein Mitglied dieser Gruppen ist. Liste: *Gruppennamen*	*Nicht zutreffend*

Berichtsabschnitt: Richtlinie 'Automatische Bereitstellung des Stammordners' wird ausgeführt

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Der Stammordner ist dem Buchstaben '*Buchstabe*' zugeordnet und mit dem Pfad '*UNC-Pfad*' in Active Directory verbunden.	*Nicht zutreffend*
• Der Stammordner '*Name*' soll auf dem Dateiserver erstellt werden.	*Nicht zutreffend*
• Der Stammordner '*Name*' wird auf dem Dateiserver erstellt.	• Der Stammordner '{0}' konnte nicht auf dem Dateiserver erstellt werden. Details: *Fehlerbeschreibung*
• Benutzerberechtigungen für den Stammordner werden durch Kopieren der Berechtigungen des übergeordneten Ordners festgelegt.	• Es konnten keine Benutzerberechtigungen für den Stammordner '*Name*' auf dem Dateiserver festgelegt werden. Details: *Fehlerbeschreibung*
• Der Stammordnerbenutzer wird als Besitzer des Stammordners festgelegt.	• Es konnten keine Benutzerberechtigungen für den Stammordner '*Name*' auf dem Dateiserver festgelegt werden. Details: *Fehlerbeschreibung*
• Die Benutzerberechtigungsoption 'Änderungszugriff erteilen' wird auf den Stammordner angewandt.	• Es konnten keine Benutzerberechtigungen für den Stammordner '*Name*' auf dem Dateiserver festgelegt werden. Details: *Fehlerbeschreibung*
• Die Benutzerberechtigungsoption 'Vollzugriff erteilen' wird auf den Stammordner angewandt.	• Es konnten keine Benutzerberechtigungen für den Stammordner '*Name*' auf dem Dateiserver festgelegt werden. Details: *Fehlerbeschreibung*
• Der Stammordner '*Name*' soll in '*neuer Name*' auf dem Dateiserver umbenannt werden.	*Nicht zutreffend*
• Der Stammordner '*Name*' wird in '*neuer Name*' auf dem Dateiserver umbenannt.	• Der Stammordner '*Name*' kann nicht in '*neuer Name*' auf dem Dateiserver umbenannt werden. Details: *Fehlerbeschreibung*
• Die Stammfreigabe '*Name*' soll auf dem Dateiserver erstellt werden.	*Nicht zutreffend*
• Die Stammfreigabe '*Name*' wird auf dem Dateiserver erstellt.	• Die Stammfreigabe '*Name*' kann nicht auf dem Dateiserver erstellt werden. Details: *Fehlerbeschreibung*
• Die Benutzerbegrenzung wird gesetzt, um nicht mehr als '*Name*' Benutzern gleichzeitig die Verbindung zur Stammfreigabe zu erlauben.	*Nicht zutreffend*
• Die Benutzerbegrenzung ist so gesetzt, dass der maximalen Anzahl von Benutzern gleichzeitig die Verbindung zur Stammfreigabe möglich ist.	*Nicht zutreffend*

Berichtsabschnitt: Richtlinie „Erzeugung und Validierung von Eigenschaften" wird ausgeführt

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Die Eigenschaft '*Name*' wird auf '*Wert*' gesetzt.	*Nicht zutreffend*
• Die Eigenschaft '*Name*' wird entfernt (gelöscht).	*Nicht zutreffend*

Berichtsabschnitt: Richtlinienskript '*Name*' wird ausgeführt

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Das folgende Berichtselement wird auf den Richtlinientyp „Skriptausführung" angewandt.	
• Das Richtlinienskript '*Name*' wurde erfolgreich abgeschlossen.	• *Von der Richtlinie zurückgegebene Fehlermeldung* Details: *Fehlerbeschreibung* *Die Standardfehlermeldung lautet wie folgt:* • Die Richtlinie „Skriptausführung" hat bei der Ausführung von Skript '*Name*' einen Fehler festgestellt. Details: *Fehlerbeschreibung*

Berichtsabschnitt: Richtlinienskript '*Name*' wird ausgeführt

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Das folgende Berichtselement wird auf den Richtlinientyp „Skriptausführung" angewandt.	
• Das Richtlinienskript '*Name*' wurde erfolgreich abgeschlossen.	• *Von der Richtlinie zurückgegebene Fehlermeldung* Details: *Fehlerbeschreibung* *Die Standardfehlermeldung lautet wie folgt:* • Die Richtlinie „Skriptausführung" hat bei der Ausführung von Skript '*Name*' einen Fehler festgestellt. Details: *Fehlerbeschreibung*

Berichtselemente der internen Richtlinie von ActiveRoles

Die internen Richtlinien von ActiveRoles dienen hauptsächlich zur Ausführung von Exchange-Empfänger-Verwaltungsaufgaben, wie etwa die Aufgabe der Erstellung eines Postfachs oder die Aufgabe der Einrichtung einer E-Mail-Adresse für eine Gruppe. Diese Richtlinien werden durch die interne Logik von ActiveRoles ausgelöst und können vom Administrator nicht konfiguriert werden. ActiveRoles führt die internen Richtlinien nach Bedarf der bestimmten Vorgangsanforderung aus. Wenn zum Beispiel eine Anforderung zur Erstellung eines Postfach-fähigen Benutzerkontos verarbeitet wird, so löst ActiveRoles eine interne Richtlinie aus, die alle Aktionen ausführt, die für die Erstellung eines Benutzerpostfaches auf dem Exchange-Server erforderlich sind.

In den folgenden Tabellen sind die möglichen Berichtselemente aufgelistet. Es ist eine Tabelle pro Berichtsabschnitt vorhanden. Die Elemente in den einzelnen Abschnitten beschreiben die Ergebnisse der Aktionen, die in Übereinstimmung mit der entsprechenden internen Richtlinie ausgeführt wurden. Berichtselemente enthalten außerdem Informationen zum Erfolg oder Fehler jeder Richtlinienaktion. Bei einem Fehler enthält das Berichtselement eine Fehlerbeschreibung.

Nicht alle aufgelisteten Elemente müssen notwendigerweise in einem Bericht enthalten sein. Ein aktueller Bericht umfasst nur Berichtselemente, die den Richtlinien entsprechen, die ActiveRoles bei der Verarbeitung der Vorgangsanforderung ausführt.

Berichtsabschnitt: Benutzerpostfach wird erstellt

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Das Benutzerpostfach '*Name*' wird erstellt.	• Das Benutzerpostfach '*Name*' kann nicht erstellt werden. Details: *Fehlerbeschreibung*
• Das Legacypostfach '*Name*' wird erstellt.	• Das Legacypostfach '*Name*' kann nicht erstellt werden. Details: *Fehlerbeschreibung*
• Der Postfachalias wird auf '*Alias*' gesetzt.	*Nicht zutreffend*
• Die Postfachdatenbank wird auf '*Datenbankname*' gesetzt.	*Nicht zutreffend*
• Die folgenden Postfacheigenschaften sind gesetzt. Liste: *Eigenschaftsnamen und -werte*	• Die folgenden Postfacheigenschaften können nicht festgelegt werden. Liste: *Eigenschaftsnamen und Fehlerbeschreibung*

Berichtsabschnitt: Verknüpftes Postfach wird erstellt

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Das verknüpfte Postfach '*Name*' wird erstellt.	• Das verknüpfte Postfach '*Name*' kann nicht erstellt werden. Details: *Fehlerbeschreibung*
• Das Legacypostfach '*Name*' wird erstellt.	• Das Legacypostfach '*Name*' kann nicht erstellt werden. Details: *Fehlerbeschreibung*
• Der Postfachalias wird auf '*Alias*' gesetzt.	*Nicht zutreffend*
• Die Postfachdatenbank wird auf '*Datenbankname*' gesetzt.	*Nicht zutreffend*
• Das Postfach ist mit dem externen Konto '*Name*' verknüpft.	*Nicht zutreffend*
• Die folgenden Postfacheigenschaften sind gesetzt. Liste: *Eigenschaftsnamen und -werte*	• Die folgenden Postfacheigenschaften können nicht festgelegt werden. Liste: *Eigenschaftsnamen und Fehlerbeschreibung*

Berichtsabschnitt: Gerätepostfach wird erstellt

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Das Gerätepostfach '*Name*' wird erstellt.	• Das Gerätepostfach '*Name*' kann nicht erstellt werden. Details: *Fehlerbeschreibung*
• Der Postfachalias wird auf '*Alias*' gesetzt.	*Nicht zutreffend*
• Die Postfachdatenbank wird auf '*Datenbankname*' gesetzt.	*Nicht zutreffend*
• Die folgenden Postfacheigenschaften sind gesetzt. Liste: *Eigenschaftsnamen und -werte*	• Die folgenden Postfacheigenschaften können nicht festgelegt werden. Liste: *Eigenschaftsnamen und Fehlerbeschreibungen*

Berichtsabschnitt: Raumpostfach wird erstellt

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Das Raumpostfach '*Name*' wird erstellt.	• Das Raumpostfach '*Name*' kann nicht erstellt werden. Details: *Fehlerbeschreibung*
• Der Postfachalias wird auf '*Alias*' gesetzt.	*Nicht zutreffend*
• Die Postfachdatenbank wird auf '*Datenbankname*' gesetzt.	*Nicht zutreffend*
• Die folgenden Postfacheigenschaften sind gesetzt. Liste: *Eigenschaftsnamen und -werte*	• Die folgenden Postfacheigenschaften können nicht festgelegt werden. Liste: *Eigenschaftsnamen und Fehlerbeschreibung*

Berichtsabschnitt: Gemeinsam genutztes Postfach wird erstellt

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Das gemeinsam genutzte Postfach '*Name*' wird erstellt.	• Das gemeinsam genutzte Postfach '*Name*' kann nicht erstellt werden. Details: *Fehlerbeschreibung*
• Der Postfachalias wird auf '*Alias*' gesetzt.	*Nicht zutreffend*
• Die Postfachdatenbank wird auf '*Datenbankname*' gesetzt.	*Nicht zutreffend*
• Das gemeinsam genutzte Postfach ist so konfiguriert, dass es den folgenden Benutzern die Verwendung dieses Postfachs ermöglicht. Liste: *Benutzernamen*	*Nicht zutreffend*
• Die folgenden Postfacheigenschaften sind gesetzt. Liste: *Eigenschaftsnamen und -werte*	• Die folgenden Postfacheigenschaften können nicht festgelegt werden. Liste: *Eigenschaftsnamen und Fehlerbeschreibung*

Berichtsabschnitt: Postfach wird verschoben

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
Die folgenden Elemente finden bei Postfachverschiebungsvorgängen auf Exchange 2007 oder früher Anwendung	
• Das Postfach '*Name*' wurde von der Datenbank '*Datenbankname*' in die Datenbank '*Datenbankname*' verschoben.	• Das Postfach '*Name*' kann nicht verschoben werden. Details: *Fehlerbeschreibung*
Die folgenden Elemente finden bei Postfachverschiebungsvorgängen auf Exchange 2010 oder später Anwendung	
• Die Postfachverschiebungsanforderung für das Postfach '*Name*' wird erstellt.	• Die Postfachverschiebungsanforderung für Postfach '*Name*' kann nicht erstellt werden. Details: *Fehlerbeschreibung*
• Das Postfach wird von Datenbank '*Datenbankname*' in Datenbank '*Datenbankname*' verschoben.	*Nicht zutreffend*

Berichtsabschnitt: Postfach wird gelöscht

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Das Postfach '*Name*' wird gelöscht.	*Nicht zutreffend*

Berichtsabschnitt: Exchange-Attribute werden entfernt

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Die folgenden Exchange-Attribute werden aus '*Name*' entfernt. Liste: *Attributnamen*	*Nicht zutreffend*

Berichtsabschnitt: Postfach wird für Unified Messaging aktiviert

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Das Postfach '*Name*' ist für Unified Messaging aktiviert.	*Nicht zutreffend*
• Die folgende Unified Messaging-Postfachrichtlinie ist dem Postfach zugewiesen: '*Richtlinienname*'	*Nicht zutreffend*
• Die folgenden Unified Messaging-Postfacheigenschaften sind gesetzt. Liste: *Eigenschaftsnamen und -werte*	*Nicht zutreffend*

Berichtsabschnitt: Unified Messaging für Postfach wird deaktiviert

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Unified Messaging ist für das Postfach '*Name*' deaktiviert.	*Nicht zutreffend*

Berichtsabschnitt: Unified Messaging-PIN wird zurückgesetzt

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Die Unified Messaging-PIN für das Postfach '*Name*' wird zurückgesetzt.	*Nicht zutreffend*

Berichtsabschnitt: E-Mail-Adresse für Gruppe wird erstellt

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Es wird eine E-Mail-Adresse für die Gruppe '*Name*' erstellt. Die Gruppe ist jetzt E-Mail-aktiviert.	• Es kann keine E-Mail-Adresse für Gruppe '*Name*' erstellt werden. Details: *Fehlerbeschreibung*
• Der E-Mail-Alias wird auf '*Alias*' gesetzt.	*Nicht zutreffend*
• Die folgenden Eigenschaften der Gruppe sind gesetzt. Liste: *Eigenschaftsnamen und -werte*	*Nicht zutreffend*

Berichtsabschnitt: Abfragebasierte Verteilergruppe wird erstellt

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Die abfragebasierte Verteilergruppe '*Name*' wird erstellt.	• Die abfragebasierte Verteilergruppe '*Name*' kann nicht konfiguriert werden. Details: *Fehlerbeschreibung*
• Der E-Mail-Alias wird auf '*Alias*' gesetzt.	*Nicht zutreffend*
• Die folgenden Eigenschaften der Gruppe sind gesetzt. Liste: *Eigenschaftsnamen und -werte*	*Nicht zutreffend*

Berichtsabschnitt: E-Mail-Adresse für Benutzer wird erstellt

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Es wird eine E-Mail-Adresse für Benutzer '*Name*' erstellt. Der Benutzer ist jetzt E-Mail-aktiviert.	• Es kann keine E-Mail-Adresse für Benutzer '*Name*' erstellt werden. Details: *Fehlerbeschreibung*
• Der E-Mail-Alias wird auf '*Alias*' gesetzt.	*Nicht zutreffend*
• Die folgenden Eigenschaften des Benutzerkontos sind gesetzt. Liste: *Eigenschaftsnamen und -werte*	*Nicht zutreffend*

Berichtsabschnitt: E-Mail-Adresse für Kontakt wird erstellt

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Es wird eine E-Mail-Adresse für den Kontakt '*Name*' erstellt. Der Kontakt ist jetzt E-Mail-aktiviert.	• Es kann keine E-Mail-Adresse für den Kontakt '*Name*' erstellt werden. Details: *Fehlerbeschreibung*
• Der E-Mail-Alias wird auf '*Alias*' gesetzt.	*Nicht zutreffend*
• Die folgenden Eigenschaften des Kontakts sind gesetzt. Liste: *Eigenschaftsnamen und -werte*	*Nicht zutreffend*

Berichtsabschnitt: E-Mail-Adresse für Gruppe wird gelöscht

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Die E-Mail-Adresse für die Gruppe '*Name*' wird gelöscht. Die Gruppe ist nicht mehr E-Mail-aktiviert.	*Nicht zutreffend*

Berichtsabschnitt: E-Mail-Adresse für Benutzer wird gelöscht

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Die E-Mail-Adresse für Benutzer '*Name*' wird gelöscht. Der Benutzer ist nicht mehr E-Mail-aktiviert.	*Nicht zutreffend*

Berichtsabschnitt: E-Mail-Adresse für Kontakt wird gelöscht

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Die E-Mail-Adresse für den Kontakt '*Name*' wird gelöscht. Der Kontakt ist nicht mehr E-Mail-aktiviert.	*Nicht zutreffend*

Berichtsabschnitt: Das Benutzerpostfach wird in ein verknüpftes Postfach umgewandelt

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Das Benutzerpostfach '*Name*' wird in ein verknüpftes Postfach umgewandelt.	*Nicht zutreffend*
• Das Postfach ist mit dem externen Konto '*Name*' verknüpft.	*Nicht zutreffend*

Berichtsabschnitt: Das verknüpfte Postfach wird in ein Benutzerpostfach umgewandelt

BERICHTSELEMENT (ERFOLG)	BERICHTSELEMENT (FEHLER)
• Das verknüpfte Postfach '*Name*' wird in ein Benutzerpostfach umgewandelt.	*Nicht zutreffend*
• Die Verknüpfung des Postfachs mit dem externen Konto '*Name*' wird aufgehoben. Das externe Konto kann nicht mehr auf das Postfach zugreifen.	*Nicht zutreffend*

Untersuchen von Benutzeraktivitäten

Im Änderungsverlaufsprotokoll können Sie auch die Änderungen untersuchen, die ein bestimmter Benutzer an Verzeichnisdaten vorgenommen hat, d.h. die Verwaltungsaktivitäten des Benutzers. Die Verwaltungsaktivität-Verweildauer hängt von der Konfiguration des Änderungsverfolgungsprotokolls ab (siehe „Richtlinie für die Änderungsnachverfolgung" weiter oben in diesem Kapitel).

Um anzuzeigen, welche Änderungen ein bestimmter Benutzer vorgenommen hat, klicken Sie auf der Quest One ActiveRoles-Konsole mit der rechten Maustaste auf das Benutzerobjekt und klicken Sie dann auf **Benutzeraktivität**.

Standardmäßig werden im Fenster **Benutzeraktivität** nur grundlegende Optionen angezeigt. Sie können weitere Optionen anzeigen, indem Sie auf das Plus-Zeichen (+) in der oberen linken Ecke neben der ersten Spaltenüberschrift klicken.

Im Fenster **Benutzeraktivität** finden Sie die folgenden Informationen:

- **Name.** Der Name des Objekts, für das Sie den Änderungsverlauf untersuchen.
- **Angefordert.** Datum und Uhrzeit der angeforderten Änderungen.
- **Abgeschlossen.** Datum und Uhrzeit der übernommenen Änderungen.
- **Eigenschaften.** Die Eigenschaften des geänderten Objekts, einschließlich Informationen über die geänderten Eigenschaftswerte.
- **Status.** Gibt an, ob die angeforderten Änderungen übernommen wurden (Status ABGESCHLOSSEN) oder die Genehmigung abgewartet wird (Status AUSSTEHEND).

Das Fenster enthält außerdem die gleichen zusätzlichen Abschnitte wie das Fenster **Änderungsverlauf** (siehe Untersuchen des Änderungsverlaufs).

12

Berechtigungsprofil

- Verstehen des Berechtigungsprofils
- Konfiguration des Berechtigungsprofils
- Anzeigen des Berechtigungsprofils

Verstehen des Berechtigungsprofils

Das Berechtigungsprofil umfasst eine Liste von Berechtigungen, die jeweils die Befugnis für den Zugriff, die Nutzung oder die Verwaltung einer bestimmten Informationsressource darstellen. Eine Ressource kann ein einzelnes Objekt im Verzeichnis sein, z. B. ein Benutzer, eine Gruppe, ein Kontakt oder ein Computerobjekt. Es kann sich auch um eine Server-basierte Ressource handeln, z. B. um ein Exchange-Postfach, um den Startordner eines Benutzers, um eine Web-Anwendung oder um eine freigegebene Netzwerkdatei. Bei einer Server-basierten Ressource liegt die Berechtigung in der Regel in Form von Benutzerattributen vor oder stammt aus der Mitgliedschaft in einer bestimmten Gruppe. Bei einem Verzeichnisobjekt bezieht sich die Berechtigung auf die Verwaltungs- oder Eigentümerrechte zu diesem Objekt.

Quest One ActiveRoles bietet die Möglichkeit zur Anzeige des Berechtigungsprofils eines bestimmten Benutzers in der Quest One ActiveRoles-Konsole und über Web Interface. Das Berechtigungsprofil wird als konfigurierbarer Bericht implementiert, der Informationen zu jenen Ressourcen anzeigt, zu denen ein Benutzer berechtigt ist. Die Konfiguration des Berechtigungsprofils gibt an, welche Ressourcen aufgelistet werden müssen und welche Informationen zu den Ressourcen im Bericht enthalten sein müssen. Quest One ActiveRoles bietet effektive Kontrollen zur Verwaltung der Konfiguration des Berechtigungsprofils.

Das Berechtigungsprofil eines Benutzers ist im Grunde eine Liste von Informationsressourcen, zu denen der Benutzer berechtigt ist. Eine Ressource kann folgende Formen annehmen:

- Eine persönliche Ressource, z. B. das Postfach des Benutzers, sein Startordner, ein Konto für Office Communications Server oder ein Unix-fähiges Konto.
- Eine freigegebene, netzwerkbasierte Ressource, z. B. eine Web-Anwendung oder eine freigegebene Netzwerkdatei, auf die der Benutzer zugreifen darf.
- Eine verwaltete Ressource, z. B. eine Gruppen- oder Verteilungsliste-, für die der Benutzer als Verwalter oder Eigentümer verantwortlich ist.

Die Art und Weise, in der ein Benutzer für eine Ressource berechtigt wird, hängt von der Art der Ressource ab:

- Bei einer persönlichen Ressource liegt die Berechtigung in Form bestimmter Attribute des Benutzerkontos im Verzeichnis vor.
- Bei einer freigegebenen Ressource wird die Berechtigung durch Hinzufügen des Benutzers zu einer bestimmten Sicherheitsgruppe im Active Directory gewährt.
- Bei einer verwalteten Ressource wird die Berechtigung durch Zuweisen der Verwalter- oder Eigentümerrolle für ein bestimmtes Objekt in Active Directory gewährt.

Die Erstellung des Berechtigungsprofils eines Benutzers erfolgt durch Anwenden der Berechtigungsregeln auf die Berechtigungszielobjekte des Benutzers. Entspricht ein Berechtigungszielobjekt den Berechtigungsregeln einer bestimmten Ressource, gilt der Benutzer als berechtigt, und Informationen zur Ressource werden im Berechtigungsprofil angezeigt. Das Berechtigungs-Zielobjekt kann einem der nachfolgend aufgeführten Typen entsprechen:

- Das Benutzerkonto in Active Directory. Dieses Objekt wird zur Ermittlung der persönlichen Ressourcen verwendet, für die der Benutzer berechtigt ist.
- Eine Active Directory-Gruppe, in der der Benutzer Mitglied ist. Dieses Objekt wird zur Ermittlung der freigegebenen Ressourcen verwendet, für die der Benutzer berechtigt ist.
- Ein Active Directory-Objekt, dem der Benutzer als Verwalter oder Eigentümer zugewiesen ist. Dieses Objekt wird zur Ermittlung der verwalteten Ressourcen verwendet, für die der Benutzer berechtigt ist.

Quest One ActiveRoles speichert die Berechtigungsregeln in Konfigurationsobjekten (Berechtigungsprofilspezifizierer). Diese Objekte sind von grundlegender Bedeutung für das Erstellen und Präsentieren des Berechtigungsprofils.

Informationen zu Berechtigungsprofilspezifizierern

In Quest One ActiveRoles sind Berechtigungsprofilspezifizierer Konfigurationsobjekte, die das Erstellen und Präsentieren des Berechtigungsprofils regeln. Jeder Spezifizierer enthält Informationen zu einer einzigen Ressource, mit denen Quest One ActiveRoles ermitteln kann, ob ein bestimmter Benutzer für eine Ressource berechtigt ist und (sofern eine Berechtigung vorliegt), welche Informationen zu dieser Ressource in das Berechtigungsprofil des Benutzers aufgenommen werden sollen.

Ein Berechtigungsprofilspezifizierer enthält die folgenden Informationen:

- **Berechtigungsart.** Definiert eine Möglichkeit, wie der Benutzer für die Ressource berechtigt wird.
- **Berechtigungsregeln.** Bietet eine Möglichkeit zur Ermittlung, ob ein Benutzer für eine Ressource berechtigt ist.
- **Ressourcenanzeige.** Definiert, wie die Ressource im Berechtigungsprofil dargestellt wird.

In den folgenden Abschnitten werden alle diese Informationsblöcke ausführlich beschrieben.

Berechtigungsart

Die Einstellung für die Berechtigungsart soll einfach das Berechtigungszielobjekt definieren. Dies ist das Objekt, auf das Quest One ActiveRoles beim Erstellen Berechtigungsprofils die Berechtigungsregeln anwendet. Berechtigungsarten können danach klassifiziert werden, wie eine Benutzerberechtigung zu einer Ressource konfiguriert wird:

- **Persönliche Ressourcenberechtigung.** Konfiguration durch Definieren bestimmter Attribute des Benutzerkontos selbst. In diesem Fall übernimmt das Benutzerkonto die Rolle des Berechtigungszielobjekts.
- **Berechtigung für freigegebene Ressource.** Wird durch Hinzufügen des Benutzers zu einer bestimmten Sicherheitsgruppe konfiguriert. In diesem Fall übernimmt die Gruppe die Rolle des Berechtigungszielobjekts.
- **Berechtigung für verwaltete Ressource.** Konfiguriert durch Zuweisen des Benutzers zur Manager- oder Eigentümerrolle für ein bestimmtes Objekt. In diesem Fall übernimmt das Objekt, das sich unter der Verwaltung oder im Besitz des Benutzers befindet, die Rolle des Berechtigungszielobjekts.

In der folgenden Tabelle werden die verfügbaren Berechtigungsarten zusammengefasst.

TYP	KONFIGURATION	ZIELOBJEKT
Berechtigung für persönliche Ressource	Das Benutzerkonto weist bestimmte, ressourcenspezifische Attribute im Verzeichnis auf.	Das Benutzerkonto
Berechtigung für freigegebene Ressource	Das Benutzerkonto gehört zu einer bestimmten Sicherheitsgruppe in Active Directory.	Die Benutzergruppe
Berechtigung für eine verwaltete Ressource	Das Benutzerkonto wird als primärer Eigentümer (Manager) oder als sekundärer Eigentümer eines bestimmten Objekts im Verzeichnis genannt.	Das Objekt, das sich unter der Verwaltung oder im Besitz des Eigentümers befindet

Berechtigungsregeln

Bei der Erstellung des Berechtigungsprofils eines Benutzers verwendet Quest One ActiveRoles die Berechtigungsregeln eines Spezifizierers, um zu ermitteln, ob der Benutzer für die vom Spezifizierer dargestellte Ressource berechtigt ist. Die Regeln werden mithilfe des Berechtigungszielobjekts evaluiert. Entspricht das Objekt den Regeln, betrachtet Quest One ActiveRoles den Benutzer als für die Ressource berechtigt und fügt Informationen zur Ressource in das Berechtigungsprofil des Benutzers ein.

Berechtigungsregeln können wie folgt nach Regelbedingungen klassifiziert werden:

- **Expliziter Ausschluss.** Die Regelbedingung umfasst eine Liste von Verzeichnisobjekten. Ist das Berechtigungszielobjekt in dieser Liste enthalten, wird davon ausgegangen, dass es nicht den Regeln entspricht.
- **Expliziter Einschluss.** Die Regelbedingung umfasst eine Liste von Verzeichnisobjekten. Ist das Berechtigungszielobjekt in dieser Liste enthalten, wird davon ausgegangen, dass es den Regeln entspricht.
- **Filterbasierter Ausschluss.** Die Regelbedingung umfasst einen oder mehrere Filter, die bestimmte Anforderungen an die Position und die Eigenschaften eines Objekts darstellen. Erfüllt ein Berechtigungsobjekt die Bedingungen mindestens eines Filters, wird davon ausgegangen, dass es nicht den Regeln entspricht.
- **Filterbasierter Einschluss.** Die Regelbedingung umfasst einen oder mehrere Filter, die bestimmte Anforderungen an die Position und die Eigenschaften eines Objekts darstellen. Erfüllt ein Berechtigungsobjekt die Bedingungen mindestens eines Filters, wird davon ausgegangen, dass es den Regeln entspricht.

Details zur Anwendung von Berechtigungsregeln durch Quest One ActiveRoles finden Sie unter Informationen zum Verfahren zur Erstellung von Berechtigungsprofilen weiter hinten in diesem Dokument.

Ressourcenanzeige

Für jede Ressource, die in das Berechtigungsprofil aufgenommen werden soll, wendet Quest One ActiveRoles Berechtigungsregeln an, um den jeweiligen Spezifizierer zu ermitteln. Anschließend werden die Regeln zur Ressourcenanzeige dieses Spezifizierers verwendet, um jenen Abschnitt des Berechtigungsprofils zu erstellen, der Informationen zur Ressource enthält.

Die Einstellungen zur Ressourcenanzeige umfassen:

- **Ressourcenartsymbol.** Grafik zur Unterscheidung der Ressourcenart im Berechtigungsprofil
- **Ressourcenartname.** Zeichenfolge zur Unterscheidung der Ressourcenart im Berechtigungsprofil
- **Ressourcen-Benennungsattribut.** Attribut des Berechtigungszielobjekts, dessen Wert zur Identifikation der Ressource im Berechtigungsprofil verwendet wird
- **Weitere, ressourcenbezogene Attribute.** Liste der Attribute des Berechtigungszielobjekts, deren Werte im Berechtigungsprofil angezeigt werden sollen

Der Abschnitt für eine bestimmte Ressource im Berechtigungsprofil ist in zwei Bereiche unterteilt:

- **Kopfzeile.** Enthält das Ressourcenartsymbol, den Ressourcenartnamen und den Wert des Ressourcen-Benennungsattributs
- **Details.** Listet die Namen und Werte der ressourcenbezogenen Attribute auf

Der Detailbereich kann mithilfe von HTML-Code an ein bestimmtes Attribut des Benutzerkontos angepasst werden, für das das Berechtigungsprofil erstellt wird. Der LDAP-Anzeigename des Attributs muss in edsaHTMLDetailsAttribute des Berechtigungsprofil-Spezifizierers angegeben werden. Daraufhin setzt Quest One ActiveRoles diesen HTML-Code um, anstatt die Attributliste im Detailbereich anzuzeigen.

Informationen zum Verfahren zur Erstellung von Berechtigungsprofilen

Nach der Aufforderung zur Erstellung des Berechtigungsprofils eines Benutzers führt Quest One ActiveRoles die nachfolgenden Schritte aus.

1. Vorbereiten eine Liste der Gruppen des Benutzers, d. h. eine Liste der Sicherheitsgruppen, zu denen der Benutzer direkt oder aufgrund von Verschachtelungen gehört
2. Vorbereiten einer Liste der verwalteten Objekte des Benutzers, d. h. eine Liste der Verzeichnisobjekte, für die der Benutzer als primärer Eigentümer (Manager) oder sekundärer Eigentümer eingetragen ist
3. Evaluieren der Berechtigungsregeln des Spezifizierers mithilfe des Benutzerkontos für alle Berechtigungsprofil-Spezifizierer des Typs „Berechtigung für persönliche Ressource" Entspricht das Benutzerkonto den Berechtigungsregeln, werden Informationen zur Ressource in das Berechtigungsprofil eingefügt. Dabei wird die Ressource gemäß den Einstellungen zur Ressourcendarstellung im Spezifizierer angegeben.
4. Für alle Gruppen des Benutzers werden die Berechtigungsprofil-Spezifizierer des Typs „Berechtigung für freigegebene Ressource" wie folgt angewendet:
   a) Für jeden Spezifizierer werden dessen Berechtigungsregeln mithilfe der Gruppe evaluiert.
   b) Entspricht die Gruppe eines Spezifizierers den Berechtigungsregeln, werden Informationen zur Ressource in das Berechtigungsprofil eingefügt. Dabei wird die Ressource gemäß den Einstellungen zur Ressourcendarstellung im Spezifizierer angegeben.
   c) Entspricht die Gruppe den Berechtigungsregeln eines oder mehrerer Spezifizierer, wird der erste gefundene Spezifizierer angewendet, wie übrigen werden ignoriert.
5. Für alle verwalteten Objekte des Benutzers werden die Berechtigungsprofil-Spezifizierer des Typs „Berechtigung für verwaltete Ressource" wie folgt angewendet:
   a) Für jeden Spezifizierer werden dessen Berechtigungsregeln mithilfe des verwalteten Objekts evaluiert.
   b) Entspricht das verwaltete Objekt eines Spezifizierers den Berechtigungsregeln, werden Informationen zur Ressource in das Berechtigungsprofil eingefügt. Dabei wird die Ressource gemäß den Einstellungen zur Ressourcendarstellung im Spezifizierer angegeben.
   c) Entspricht das verwaltete Objekt den Berechtigungsregeln eines oder mehrerer Spezifizierer, wird der erste gefundene Spezifizierer angewendet, wie übrigen werden ignoriert.

Berechtigungsregeln spielen eine wichtige Rolle bei der Erstellung des Berechtigungsprofils. Die Berechtigungsregeln legen fest, ob Quest One ActiveRoles einen Benutzer als für eine Ressource berechtigt ansieht und somit Informationen zur Ressource in das Berechtigungsprofil dieses Benutzers einfügt. Beim Evaluieren von Berechtigungsregeln zu einem bestimmten Objekt führt Quest One ActiveRoles die folgenden Schritte aus.

1. Anwenden der Regeln für expliziten Ausschluss Ist das Objekt in der Liste der ausgeschlossenen Objekte enthalten, werden die übrigen Regeln ignoriert, und das Objekt wird als von den Regeln abweichend markiert. Andernfalls folgt der nächste Schritt.
2. Anwenden der Regeln für expliziten Einschluss Ist das Objekt in der Liste der eingeschlossenen Objekte enthalten, werden die übrigen Regeln ignoriert, und das Objekt wird als den Regeln entsprechend markiert. Andernfalls folgt der nächste Schritt.
3. Anwenden der Regeln für filterbasierten Ausschluss Erfüllt das Objekt die Regelbedingung, werden die übrigen Regeln ignoriert, und das Objekt wird als von den Regeln abweichend markiert. Andernfalls folgt der nächste Schritt.
4. Anwenden der Regeln für filterbasierten Einschluss Erfüllt das Objekt die Regelbedingung, wird des als den Regeln entsprechend markiert.

Es kann vorkommen, dass das Berechtigungszielobjekt den Berechtigungsregeln mehrerer Spezifizierer entspricht. In diesem Fall muss Quest One ActiveRoles einen einzelnen Spezifizierer aus jenen auswählen, die dem Berechtigungszielobjekt entsprechen. Dies geschieht wie folgt:

1. Das Attribut edsaPriority jedes Spezifizierers wird geprüft. Es wird nach Spezifizierern gesucht, bei denen edsaPriority nicht gesetzt ist. Wird kein solcher Spezifizierer gefunden, weiter mit Schritt 3. Wird ein Spezifizierer gefunden, wird dieser angewendet. Andernfalls weiter mit Schritt 2.
2. Die Spezifizierer ohne edsaPriority werden in aufsteigender alphanumerischer Reihenfolge nach Name sortiert. Dann wird der erste Spezifizierer angewendet. Die Schritte 3-4 werden nicht ausgeführt.
3. Die Spezifizierer mit dem geringsten Wert für edsaPriority werden ausgewählt. Weist ein einziger Spezifizierer den geringsten Wert für edsaPriority auf, wird dieser angewendet. Andernfalls folgt der nächste Schritt.
4. Die Spezifizierer mit dem geringsten Wert für edsaPriority werden in aufsteigender alphanumerischer Reihenfolge nach Name sortiert. Dann wird der erste Spezifizierer angewendet.

Hierbei ist zu beachten, dass Spezifizierer ohne edsaPriority Vorrang vor Spezifizierern mit einem Wert für edsaPriority haben.

Hat Quest One ActiveRoles einen einzelnen Spezifizierer für die Berechtigung zu einer Ressource identifiziert, werden die Einstellungen zur Ressourcendarstellung des Spezifizierers zur Erstellung eines Abschnitts im Berechtigungsprofil verwendet, der Informationen zur Ressource darstellt. Entsprechen mehrere Ressourcen einem bestimmten Spezifizierer, werden die Abschnitte zu diesen Ressourcen in einem erweiterbaren Block gruppiert, um die Übersicht des Berechtigungsprofils zu wahren.

Konfiguration des Berechtigungsprofils

In Quest One ActiveRoles bieten Berechtigungsprofil-Spezifizierer die Möglichkeit, die Berechtigungsdefinition für eine bestimmte Ressource in einem einzigen Objekt zu speichern. Berechtigungsprofil-Spezifizierer bestimmen den Inhalt des Berechtigungsprofils.

Bei der Erstellung des Berechtigungsprofils eines Benutzers verwendet Quest One ActiveRoles die Berechtigungsprofil-Spezifizierer, um jene Ressourcen zu ermitteln, für die der Benutzer berechtigt ist. Außerdem wird so festgestellt, welche Informationen zu den Ressourcen im Berechtigungsprofil angezeigt werden.

Quest One ActiveRoles wird mit einer Sammlung vordefinierter Spezifizierer ausgeliefert, sodass Administratoren weitere Spezifizierer erstellen oder vorhandene ändern können. Sie können die folgenden Anweisungen verwenden, um Berechtigungsprofil-Spezifizierer zu erstellen oder zu ändern:

- Erstellen von Berechtigungsprofil-Spezifizierern
- Ändern von Berechtigungsprofil-Spezifizierern

Eine Liste der vordefinierten Spezifizierer finden Sie unter Vordefinierte Spezifizierer.

Erstellen von Berechtigungsprofil-Spezifizierern

Quest One ActiveRoles speichert Berechtigungsprofil-Spezifizierer im Container **Berechtigungsprofil-Spezifizierer**. Sie können auf diesen Container in der **-Konsole zugreifen, indem Sie den Zweig** Konfiguration/Server-KonfigurationQuest One ActiveRoles der Konsolenstruktur erweitern.

So erstellen Sie einen Berechtigungsprofil-Spezifizierer:

1. Klicken Sie in der Konsolenstruktur unter **Konfiguration/Server-Konfiguration/ Richtlinienarten** mit der rechten Maustaste auf den Richtlinientypcontainer, in dem Sie einen neuen Container erstellen möchten, und wählen Sie dann **Neu | Richtlinientypcontainer**.

   *Wenn Sie zum Beispiel einen neuen Container im Root-Container erstellen möchten, klicken Sie mit der rechten Maustaste auf **Berechtigungsprofil-Spezifizierer**.*

2. Geben Sie im Assistenten „Neues Objekt – Berechtigungsprofil-Spezifizierer" einen Namen und optional eine Beschreibung für den neuen Spezifizierer ein.

   Mit dem Namen und der Beschreibung wird das Spezifizierer-Objekt in der Quest One ActiveRoles-Konsole identifiziert.

3. Klicken Sie auf **Weiter**.
4. Wählen Sie die gewünschte Berechtigungsart:
   - Wählen Sie die Option **Benutzerattribute**, wenn die Tatsache, dass ein Benutzer für die Ressource berechtigt ist, auf bestimmten Attributeinstellungen des Benutzerkontos in Active Directory basiert. Dies ist beispielsweise die Art der Berechtigung für ein Exchange-Postfach oder für einen Startordner.
   - Wählen Sie die Option **Gruppenmitgliedschaft**, wenn die Tatsache, dass ein Benutzer für die Ressource berechtigt ist, auf der Mitgliedschaft des Benutzers in einer bestimmten Sicherheitsgruppe basiert.
   - Wählen Sie die Option **Manager- oder Eigentümerrolle zuweisen**, wenn die Berechtigung eines Benutzers für eine Ressource bedeutet, dass der Benutzer als Manager (primärer Eigentümer) oder sekundärer Eigentümer eines Objekts geführt wird.

5. Klicken Sie auf **Weiter**.
6. Richten Sie die Liste **Berechtigungsregeln** ein.

   In diesem Schritt definieren Sie die Kriterien, mit denen ermittelt wird, ob ein Benutzer für die Ressource berechtigt ist. Die Berechtigungsregel nimmt die Form von Bedingungen an, die das Berechtigungszielobjekt erfüllen muss, damit der Benutzer als für die Ressource berechtigt gilt und damit Informationen zur Ressource im Berechtigungsprofil des Benutzers erscheinen.

   Quest One ActiveRoles evaluiert die Berechtigungsregeln mithilfe des Berechtigungszielobjekts, wenn das Berechtigungsprofil eines Benutzers erstellt wird. Je nach Berechtigungstyp ist das Berechtigungszielobjekt:

   - Im Fall der Berechtigungsart **Benutzerattribute** das Benutzerkonto des Benutzers, dessen Berechtigungsprofil erstellt wird (Diese Berechtigungsart wird als *Berechtigung für eine persönliche Ressource* bezeichnet.)
   - Im Fall der Berechtigungsart **Gruppenmitgliedschaft** jede einzelne Gruppe, zu der der Benutzer gehört – direkt oder auf der Basis von Verschachtelungen (Diese Berechtigungsart wird als *Berechtigung für eine freigegebene Ressource* bezeichnet.)
   - Im Fall der Berechtigungsart **Zuweisung der Manager- oder Eigentümerrolle** jedes einzelne Objekt, für das der Benutzer als Manager (primärer Eigentümer) oder als sekundärer Eigentümer geführt wird. (Diese Berechtigungsart wird als *Berechtigung für eine verwaltete Ressource* bezeichnet.)

   Sie können die Berechtigungsregeln auf Basis von Objekteigenschaften definieren, z. B. danach, ob für das Objekt bestimmte Attribute gesetzt sind oder ob sich sich beim Objekt um eine Sicherheitsgruppe handelt. Die Bedingungen nehmen die Form von auf LDAP-Filtern basierten Suchkriterien an. Bei der Regelart „Einschließen" wird der Benutzer als für die Ressource berechtigt angesehen, wenn das Berechtigungszielobjekt die Suchkriterien erfüllt. Bei der Regelart „Ausschließen" wird der Benutzer als nicht für die Ressource berechtigt angesehen, wenn das Berechtigungszielobjekt die Suchkriterien erfüllt.

   Neben den filterbasierten Regeln können Sie Regeln auf Objektbasis definieren, um z. B. einzelne Objekte explizit in die Berechtigungszuweisung einzuschließen oder davon auszuschließen. Trifft Quest One ActiveRoles auf eine Regel zum Einschließen des Berechtigungszielobjekts, wird der Benutzer als für die Ressource berechtigt angesehen. Trifft Quest One ActiveRoles auf eine Regel zum Ausschließen des Berechtigungszielobjekts, wird der Benutzer als nicht für die Ressource berechtigt angesehen.

   Quest One ActiveRoles evaluiert die Berechtigungsregeln in der folgenden Reihenfolge:

   a) Expliziter Ausschluss

   b) Expliziter Einschluss

   c) Filterbasierter Ausschluss

   d) Filterbasierter Einschluss

   Entspricht das Berechtigungszielobjekt einer bestimmten Art von Regel, werden die Regelarten, die in dieser Liste unterhalb stehen, nicht angewendet. Dies bedeutet, dass Ausschlussregeln Vorrang vor Einschlussregeln haben und dass die explizite Auswahl von Objekten Vorrang vor filterbasierten Regeln hat.

   Zunächst sind keine Berechtigungsregeln konfiguriert. Dies wird als Einschlussbedingung gewertet, die für jedes Objekt WAHR ergibt. Daher wird die Berechtigung für die Ressource unabhängig von den Eigenschaften des Berechtigungszielobjekts etabliert. Sie können Berechtigungsregeln hinzufügen, um Berechtigungen auf Basis der Eigenschaften von Berechtigungszielobjekten zu kategorisieren.

Zum Hinzufügen einer Berechtigungsregel klicken Sie auf **Einschließen** oder **Ausschließen**, je nach gewünschter Regelart. Verwenden Sie dann das Dialogfeld **Berechtigungsregel konfigurieren**, um Ihre Suchkriterien anzugeben. Sie können die Suchkriterien auf exakt die gleiche Weise angeben, wie Sie dies im Dialogfeld **Suchen** tun. Führen Sie dann eine der folgenden Aktionen durch:

- Um eine Regel hinzuzufügen, die auf den von Ihnen angegebenen Suchkriterien basiert, klicken Sie auf **Regel hinzufügen**.
- Um bestimmte Objekte auszuwählen, klicken Sie auf **Jetzt suchen**, aktivieren die Kontrollkästchen in der Liste der Suchergebnisse und klicken dann auf **Auswahl hinzufügen**.

7. Klicken Sie auf **Weiter**.
8. Anzeigen oder Ändern des Symbols, das zur Unterscheidung der Ressourcenart im Berechtigungsprofil verwendet wird:
   - Anzeigen des Symbols im Bereich neben der Schaltfläche **Ändern**.
   - Wenn Sie ein anderes Symbol wählen möchten, klicken Sie auf **Ändern**, und wählen Sie die gewünschte Bilddatei.
   - Um wieder das Standardbild zu verwenden, klicken Sie auf **Standardsymbol verwenden**.
9. Geben Sie den Namen der Ressourcenart ein, die im Berechtigungsprofil angezeigt werden soll.
10. Klicken Sie auf **Auswählen**, um das Attribut des Berechtigungszielobjekts auszuwählen, dessen Wert zur Benennung der Ressource im Berechtigungsprofil verwendet wird.

    Das Ressourcenartsymbol, der Anzeigename und das Benennungsattribut werden zur Identifikation der Ressource im Berechtigungsprofil verwendet. Weist die Evaluierung der Berechtigungsregeln für einen Benutzer darauf hin, dass der Benutzer für die Ressource berechtigt ist, werden Informationen zur Ressource als separater Abschnitt im Berechtigungsprofil des Benutzers angezeigt. Die Kopfzeile des Abschnitts enthält das Ressourcenartsymbol, den Anzeigenamen der Ressourcenart und den Wert des Benennungsattributs, der aus dem Berechtigungszielobjekts abgerufen wird.
11. Klicken Sie auf **Weiter**.
12. Richten Sie die Liste der ressourcenbezogenen Attribute ein, die im Berechtigungsprofil angezeigt werden:
    - Verwenden Sie die Schaltfläche **Hinzufügen** oder **Entfernen**, um Attribute zur Liste hinzuzufügen oder aus dieser zu entfernen.
    - Klicken Sie auf **Trennung hinzufügen**, um die Attributliste im Berechtigungsprofil in Abschnitte zu unterteilen.
    - Verwenden Sie die Schaltflächen **Auf** und **Ab**, um die Reihenfolge in der Attributliste zu ändern.

    Die Attribute in der Liste werden im Berechtigungsprofil angezeigt (unter der Kopfzeile des Abschnitts, der Informationen zur Ressource enthält). Für jedes aufgeführte Attribut enthält der Abschnitt den Namen und den Wert des Attributs aus dem Berechtigungszielobjekts.
13. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Ändern von Berechtigungsprofil-Spezifizierern

Sie können einen vorhandenen Berechtigungsprofil-Spezifizierer ändern, indem Sie dessen Namen und Beschreibung, die Berechtigungsarten und Regeln, die Einstellungen für die Ressourcenanzeige und die Ressourcenattributliste ändern. Die Objekte des Berechtigungsprofil-Spezifizierers befinden sich unter **Konfiguration/Server-Konfiguration/Berechtigungsprofil-Spezifizierer** in der Quest One ActiveRoles-Konsole.

Die folgende Tabelle fasst die Änderungen zusammen, die Sie an einem vorhandenen Berechtigungsprofil-Spezifiziererobjekt vornehmen können, vorausgesetzt, dass Sie das Objekt in der Quest One ActiveRoles-Konsole gefunden haben. Sie können einen Spezifizierer auch mit den Befehlen **Deaktivieren** oder **Löschen** im Menü **Aktion** deaktivieren oder löschen. Quest One ActiveRoles ignoriert die deaktivierten Spezifizierer beim Erstellen des Berechtigungsprofils. Sie können einen deaktivierten Spezifizierer erneut aktivieren, indem Sie den Befehl **Aktivieren** verwenden, der im Menü **Aktion** für deaktivierte Spezifizierer verwendet wird.

ÄNDERUNG VON	VORGEHENSWEISE	KOMMENTAR
Name	Klicken Sie mit der rechten Maustaste auf das Objekt und klicken Sie dann auf **Umbenennen**.	Der Name wird verwendet, um das Objekt zu identifizieren. Er muss für die im selben Container enthaltenen Objekte eindeutig sein.
Beschreibung	Klicken Sie mit der rechten Maustaste auf das Objekt, klicken Sie auf **Eigenschaften** und nehmen Sie die erforderlichen Änderungen auf der Registerkarte **Allgemein** vor.	Die Beschreibung unterstützt Quest One ActiveRoles-Administratoren bei der Identifikation von Zweck und Funktion des Objekts.
Berechtigungsart	Klicken Sie mit der rechten Maustaste auf das Objekt, klicken Sie auf **Eigenschaften**, klicken Sie auf die Registerkarte **Art**, und wählen Sie die gewünschte Option aus.	Die Berechtigungsart gibt an, wie der Benutzer für die Nutzung der Ressource berechtigt ist. Der Benutzer wird folgendermaßen für die Nutzung dieser Ressource berechtigt: • **Benutzerattribute.** Berechtigung für eine persönliche Ressource, z. B. für ein Postfach oder einen Startordner, kontrolliert durch bestimmte Attribute des Benutzerkontos. • **Gruppenmitgliedschaft.** Berechtigung für eine gemeinsam genutzte Ressource, z. B. eine Web-Anwendung oder eine freigegebene Netzwerkdatei über die Mitgliedschaft in einer Sicherheitsgruppe. • **Zuweisung der Manager- oder Eigentümerrolle.** Berechtigung zum Handeln als Manager (primärer Eigentümer) oder als sekundärer Eigentümer eines Verzeichnisobjekts, wie z. B. eine Gruppe, eine Verteilerliste oder ein Computer.

ÄNDERUNG VON	VORGEHENSWEISE	KOMMENTAR
Berechtigungsregeln	Klicken Sie mit der rechten Maustaste auf das Objekt, klicken Sie auf **Eigenschaften**, klicken Sie auf die Registerkarte **Regeln**. Anschließend können Sie Berechtigungsregeln hinzufügen, entfernen oder ändern, indem Sie die Schaltflächen unter der Regelliste verwenden.	Mit den Berechtigungsregeln wird ermittelt, ob ein Benutzer für die Ressource berechtigt ist. Die Berechtigungsregel nimmt die Form von Bedingungen an, die das Berechtigungszielobjekt erfüllen muss, damit der Benutzer als für die Ressource berechtigt gilt und damit Informationen zur Ressource im Berechtigungsprofil des Benutzers erscheinen. Wenn Sie eine Berechtigungsregel hinzufügen oder ändern möchten, klicken Sie auf **Einschließen** oder **Ausschließen**, je nach der gewünschten Regelart. Sie können auch auf **Anzeigen/ Bearbeiten** klicken und das Dialogfeld **Berechtigungsregel konfigurieren** verwenden, um die Regelbedingungen zu definieren. Sie können dies in der gleichen Weise wie im Dialogfeld **Suchen** tun, um eine Suche zu konfigurieren und auszuführen. Beachten Sie, dass Sie nur filterbasierte Regeln Regeln ändern. Wenn Sie eine explizite Einschluss- oder Ausschlussregel auswählen, ist die Schaltfläche **Anzeigen/ Bearbeiten** nicht verfügbar. Sie können die Schaltfläche **Entfernen** nutzen, um eine beliebige Regel zu entfernen. Weitere Informationen finden Sie in Schritt 6 unter Erstellen von Berechtigungsprofil-Spezifizierern.
Einstellungen für die Ressourcenanzeige	Klicken Sie mit der rechten Maustaste auf das Objekt, klicken Sie auf **Eigenschaften**, klicken Sie auf die Registerkarte **Anzeigen**. Anschließend können Sie das Symbol und den Anzeigenamen der Ressourcenart und das Benennungsattribut der Ressource ändern.	Das Ressourcenartsymbol, der Anzeigename und das Benennungsattribut werden zur Identifikation der Ressource im Berechtigungsprofil verwendet. Weist die Evaluierung der Berechtigungsregeln für einen Benutzer darauf hin, dass der Benutzer für die Ressource berechtigt ist, werden Informationen zur Ressource als separater Abschnitt im Berechtigungsprofil des Benutzers angezeigt. Die Kopfzeile des Abschnitts enthält das Ressourcenartsymbol, den Anzeigenamen der Ressourcenart und den Wert des Benennungsattributs, der aus dem Berechtigungszielobjekts abgerufen wird.
Ressourcenattributliste	Klicken Sie mit der rechten Maustaste auf das Objekt, klicken Sie auf **Eigenschaften**, klicken Sie auf die Registerkarte **Attribute**. Anschließend können Sie Attribute hinzufügen, entfernen oder deren Reihenfolge ändern, indem Sie die Schaltflächen unter der Attributliste verwenden.	Auf der Registerkarte werden die Attribute des Berechtigungszielobjekts aufgelistet, die im Berechtigungsprofil angezeigt werden (unter der Kopfzeile des Abschnitts, der Informationen zur Ressource enthält). Für jedes aufgeführte Attribut enthält der Abschnitt den Namen und den Wert des Attributs aus dem Berechtigungszielobjekts.

Vordefinierte Spezifizierer

Quest One ActiveRoles wird mit einer Sammlung vordefinierter Spezifizierer ausgeliefert, die die standardmäßige Konfiguration des Ressourcenprofils definieren. Die vordefinierten Spezifizierer befinden sich im Container **Konfiguration/Server-Konfiguration/Berechtigungsprofil-Spezifizierer/Integriert** und können über die Quest One ActiveRoles-Konsole verwaltet werden. Sie können Änderungen an einem vordefinierten Spezifizierer vornehmen (siehe Ändern von Berechtigungsprofil-Spezifizierern). Sie können auch den Befehl **Deaktivieren** für den Spezifizierer aussetzen. Beachten Sie, dass vordefinierte Spezifizierer nicht gelöscht werden können.

Die vordefinierten Spezifizierer haben eine geringere Priorität als selbst erstellte Spezifizierer. Dies bedeutet, dass die Berechtigungsregeln selbst erstellter Spezifizierer zuerst evaluiert werden. Entspricht ein Berechtigungszielobjekt den Berechtigungsregeln eines vordefinierten und eines selbst definierten Spezifizierers, wird letzterer angewendet. Die Priorität der Spezifizierer wird durch die Attributeinstellung edsaPriority geregelt (siehe Informationen zum Verfahren zur Erstellung von Berechtigungsprofilen).

Die folgende Tabelle enthält Informationen zu den vordefinierten Spezifizierern. Für jeden Spezifizierer listet die Tabelle den Namen, die Beschreibung, die Berechtigungsart, die Regeln und die Einstellungen für die Ressourcenanzeige auf.

NAME UND BESCHREIBUNG	ARTEN UND REGELN	EINSTELLUNGEN FÜR DIE RESSOURCENANZEIGE
Name: Selbst – Exchange-Postfach *Beschreibung*: Gibt die Benutzerberechtigung für das Exchange-Postfach an	*Art*: Berechtigung für persönliche Ressource *Regeln*: Das Berechtigungszielobjekt ist ein Benutzerkonto für ein Exchange-Postfach.	*Name der Ressourcenart*: Exchange-Postfach *Ressourcen-Benennungsattribut*: mail *Weitere, ressourcenbezogene Attribute*: • mail • homeMDB • displayName
Name: Selbst – Startordner *Beschreibung*: Gibt die Benutzerberechtigung für den Startordner an	*Art*: Berechtigung für persönliche Ressource *Regeln*: Für das Berechtigungszielobjekt wurde das Attribut homeDirectory gesetzt.	*Name der Ressourcenart*: Startordner *Ressourcen-Benennungsattribut*: homeDirectory *Weitere, ressourcenbezogene Attribute*: • homeDirectory • homeDrive
Name: Selbst – Unix-Konto *Beschreibung*: Gibt die Benutzerberechtigung für das Unix-fähige Konto an.	*Art*: Berechtigung für persönliche Ressource *Regeln*: Für das Berechtigungsobjekt wurde das Attribut uidNumber gesetzt, UND der Wert des Attributs loginShell lautet nicht /bin/false.	*Name der Ressourcenart*: Unix-fähiges Konto *Ressourcen-Benennungsattribut*: userPrincipalName *Weitere, ressourcenbezogene Attribute*: • userPrincipalName • uidNumber • gidNumber • unixHomeDirectory • loginShell

NAME UND BESCHREIBUNG	ARTEN UND REGELN	EINSTELLUNGEN FÜR DIE RESSOURCENANZEIGE
Name: Selbst – OCS-Konto *Beschreibung*: Gibt die Benutzerberechtigung für das Office Communications Server-fähige Konto an	*Art*: Berechtigung für persönliche Ressource *Regeln*: Für das Berechtigungszielobjekt wurde das Attribut „msRTCSIP-UserEnabled" attribute auf WAHR gesetzt.	*Name der Ressourcenart*: Aktiviert für Office Communications Server *Ressourcen-Benennungsattribut*: msRTCSIP-PrimaryUserAddress *Weitere, ressourcenbezogene Attribute*: • msRTCSIP-PrimaryUserAddress • edsva-OCS-Pool
Name: Mitgliedschaft – Mitglied der Sicherheitsgruppe *Beschreibung*: Gibt die Berechtigung für eine Ressource über die Mitgliedschaft in einer Sicherheitsgruppe an.	*Art*: Berechtigung für freigegebene Ressource *Regeln*: Berechtigungszielobjekt ist eine Sicherheitsgruppe **Anmerkung:** Dieser Spezifizierer hat die geringste Priorität gemäß Attributeinstellung für edsaPriority. Daher werden die Berechtigungsregeln anderer Spezifizierer der Art „Berechtigung für freigegebene Ressource" vor den Regeln dieses Spezifizierers evaluiert.	*Name der Ressourcenart*: Mitglied der Sicherheitsgruppe *Ressourcen-Benennungsattribut*: Name *Weitere, ressourcenbezogene Attribute*: • Name • displayName • Beschreibung • info • edsvaResourceURL • managedBy • edsvaPublished • edsvaApprovalByPrimaryOwnerRequired • edsvaParentCanonicalName
Name: Mitgliedschaft – Zugriff auf SharePoint-Site *Beschreibung*: Gibt die Berechtigung für eine SharePoint-Site über die Mitgliedschaft in einer bestimmten Sicherheits-gruppe an	*Art*: Berechtigung für freigegebene Ressource *Regeln*: Das Berechtigungszielobjekt ist eine Sicherheitsgruppe mit gesetztem Attribut edsva-SP-MirrorType.	*Name der Ressourcenart*: Zugriff auf SharePoint-Site *Ressourcen-Benennungsattribut*: Name *Weitere, ressourcenbezogene Attribute*: • Name • edsva-SP-SiteName • edsva-SP-SiteURL • managedBy • edsvaPublished • edsvaApprovalByPrimaryOwnerRequired • edsvaParentCanonicalName

NAME UND BESCHREIBUNG	ARTEN UND REGELN	EINSTELLUNGEN FÜR DIE RESSOURCENANZEIGE
Name: Verwaltet von – Eigentümer der Sicherheitsgruppe *Beschreibung*: Gibt die Berechtigung für die Verwalter- oder Eigentümerrolle für eine Sicherheitsgruppe an.	*Art*: Berechtigung für eine verwaltete Ressource *Regeln*: Berechtigungszielobjekt ist eine Sicherheitsgruppe	*Name der Ressourcenart*: Eigentümer der Sicherheitsgruppe *Ressourcen-Benennungsattribut*: Name *Weitere, ressourcenbezogene Attribute*: • Name • displayName • Beschreibung • info • edsvaResourceURL • managedBy • edsvaPublished • edsvaApprovalByPrimaryOwnerRequired • edsvaParentCanonicalName
Name: Verwaltet von – Eigentümer der Verteilerliste *Beschreibung*: Gibt die Berechtigung für die Verwalter- oder Eigentümerrolle für eine Verteilergruppe an.	*Art*: Berechtigung für eine verwaltete Ressource *Regeln*: Das Berechtigungszielobjekt ist eine (Verteiler-) Gruppe für ein Exchange-Postfach.	*Name der Ressourcenart*: Eigentümer der Verteilerliste *Ressourcen-Benennungsattribut*: displayName *Weitere, ressourcenbezogene Attribute*: • displayName • mail • Beschreibung • info • managedBy • edsvaPublished • edsvaApprovalByPrimaryOwnerRequired • edsvaParentCanonicalName
Name: Verwaltet von – Besitzer des Exchange-Ressourcenpostfachs **Anmerkung:** *Beschreibung*: Gibt die Berechtigung für die Besitzerrolle für ein Raum-, Geräte- oder gemeinsam genutztes Postfach an.	*Art*: Berechtigung für eine verwaltete Ressource *Regeln*: Das Berechtigungszielobjekt ist ein Benutzerkonto zu einem Raum, einer Ausrüstungskomponente oder einem freigegebenen Postfach.	*Name der Ressourcenart*: Eigentümer des Exchange-Ressourcenpostfachs *Ressourcen-Benennungsattribut*: displayName *Weitere, ressourcenbezogene Attribute*: • displayName • edsva-MsExch-MailboxTypeDescription • mail • Beschreibung • homeMDB • edsvaParentCanonicalName

NAME UND BESCHREIBUNG	ARTEN UND REGELN	EINSTELLUNGEN FÜR DIE RESSOURCENANZEIGE
Name: Verwaltet von – Eigentümer des Exchange-Kontakts **Anmerkung:** *Beschreibung*: Gibt die Berechtigung für die Eigentümerrolle für einen Exchange-Mail-Kontakt an	*Art*: Berechtigung für eine verwaltete Ressource *Regeln*: Das Berechtigungszielobjekt ist ein Exchange-Mail-Kontakt.	*Name der Ressourcenart*: Eigentümer des Exchange-Kontakts *Ressourcen-Benennungsattribut*: displayName *Weitere, ressourcenbezogene Attribute*: • displayName • givenName • sn • mail • telephoneNumber • company • edsvaParentCanonicalName
Name: Verwaltet von – Eigentümer des Computers **Anmerkung:** *Beschreibung*: Gibt die Berechtigung für die Verwalter- oder Eigentümerrolle für einen Computer an.	*Art*: Berechtigung für eine verwaltete Ressource *Regeln*: Das Berechtigungszielobjekt ist ein Computerkonto.	*Name der Ressourcenart*: Eigentümer des Computers *Ressourcen-Benennungsattribut*: Name *Weitere, ressourcenbezogene Attribute*: • Name • dNSHostName • Beschreibung • operatingSystem • edsvaParentCanonicalName
Name: Verwaltet von – Standard *Beschreibung*: Standard-Kennzeichner für die Berechtigung zur Verwalter- oder Besitzerrolle	*Art*: Berechtigung für eine verwaltete Ressource *Regeln*: Keine Regeln definiert. Dies bedeutet, dass ein Objekt als den Berechtigungsregeln dieses Spezifizierers entsprechend angesehen wird. **Anmerkung:** Dieser Spezifizierer hat die geringste Priorität gemäß Attributeinstellung für edsaPriority. Daher werden die Berechtigungsregeln anderer Spezifizierer der Art „Berechtigung für verwaltete Ressource" vor den Regeln dieses Spezifizierers evaluiert.	*Name der Ressourcenart*: Eigentümer von *<Anzeigename der Zielobjektklasse>* *Ressourcen-Benennungsattribut*: Name *Weitere, ressourcenbezogene Attribute*: • Name • Beschreibung • edsvaParentCanonicalName

Anzeigen des Berechtigungsprofils

Sie können auf das Berechtigungsprofil eines Benutzers über die Quest One ActiveRoles-Konsole oder die Web-Schnittstelle zugreifen. Auf diese Weise können Sie schnell Ressourcen untersuchen, für die der Benutzer berechtigt ist:

- Klicken Sie in der Konsole mit der rechten Maustaste auf den Benutzer, und klicken Sie dann auf **Berechtigungsprofil**. Sie können auch auf die Schaltfläche **Berechtigungsprofil** auf der Registerkarte **Verwaltete Ressourcen** im Dialogfeld **Eigenschaften** für das Benutzerkonto klicken.
- Klicken Sie im Web-Interface auf den Benutzer, und wählen Sie **Berechtigungsprofil** aus der Befehlsliste.

Auf diese Weise wird die Seite **Berechtigungsprofil** geöffnet auf der die Ressourcen des Benutzers in erweiterbaren Blöcken nach Ressourcentyp gruppiert sind. Jeder Block kann ein Abschnitt sein, der für eine einzige Ressource steht. Er kann auch eine Reihe von Abschnitten umfassen, die jeweils für eine einzelne Ressource stehen. Es werden Ressourcen der gleichen Art gruppiert. So können z. B. die Sicherheitsgruppen, in denen der Benutzer Mitglied ist, in einem Block gruppiert werden. Hierbei wird jede Gruppe durch einen separaten Abschnitt dargestellt.

Anfangs stellt jeder Block/Abschnitt nur eine Kopfzeile dar, die folgende Elemente enthält:

- **Ressourcensymbol.** Grafik zur Unterscheidung der Ressourcenart
- **Ressourcenart.** Textzeichenfolge zur Identifikation der Ressourcenart
- **Ressourcenname.** Textzeichenfolge zur Identifikation des Ressourcennamens oder zur Anzeige, dass der Block mehrere ressourcenspezifische Abschnitte enthält.

Zum Anzeigen von Ressourcendetails klicken Sie auf die Kopfzeile eines Blocks oder eines Abschnitts.

Nach der Installation ist Quest One ActiveRoles so konfiguriert, dass das Berechtigungsprofil eines Benutzers dessen Berechtigung für Ressourcen darstellt, die in der nachfolgenden Tabelle enthalten sind. Quest One ActiveRoles-Administratoren können das Berechtigungsprofil so konfigurieren, dass Informationen zu weiteren Ressourcen angezeigt werden. Ist ein Benutzer nicht für Ressourcen einer bestimmten Art berechtigt, enthält sein Berechtigungsprofil keine Abschnitte zu dieser Ressourcenart. Verfügt ein Benutzer z. B. nicht über ein Exchange-Postfach, enthält sein Berechtigungsprofil keine Informationen zu dessen Postfach.

RESSOURCENTYP	RESSOURCENNAME	RESSOURCENDETAILS
Exchange-Postfach	E-Mail-Adresse des Postfachs	• E-Mail-Adresse • Postfachspeicher oder Datenbankposition • Anzeigename des Postfachbenutzers
Stammordner	Pfad und Name des Startordners	• Pfad und Name des Startordners • Laufwerksbuchstabe zum Startordner
Für Unix aktiviertes Konto	Hauptname des Benutzers	• Hauptname des Benutzers • Unix-Benutzerkennung (UID) • Primäre Unix-Gruppen-ID (GID) • Unix-Startverzeichnis • Unix-Login shell
Aktiviert für Office Communications Server	Live-Kommunikationsadresse	• Live-Kommunikationsadresse • Office Communications-Server oder -Pool

RESSOURCENTYP	RESSOURCENNAME	RESSOURCENDETAILS
Mitglied der Sicherheitsgruppe	Gruppenname	• Gruppenname • Gruppenanzeigename • Gruppenbeschreibung • Gruppenhinweise • Ressourcenadresse (URL) • Gruppeneinstellung „Verwaltet von" • Gruppeneinstellung „Wird veröffentlicht" • Gruppeneinstellung „Genehmigung durch Primäreigentümer erforderlich" • Gruppenposition (Einstellung „In Ordner")
Zugriff auf SharePoint-Site	Gruppenname	• Gruppenname • SharePoint-Site-Name • SharePoint-Site-Adresse (URL) • Gruppeneinstellung „Verwaltet von" • Gruppeneinstellung „Wird veröffentlicht" • Gruppeneinstellung „Genehmigung durch Primäreigentümer erforderlich" • Gruppenposition (Einstellung +„In Ordner")
Besitzer der Sicherheitsgruppe	Gruppenname	• Gruppenname • Gruppenanzeigename • Gruppenbeschreibung • Gruppenhinweise • Ressourcenadresse (URL) • Gruppeneinstellung „Verwaltet von" • Gruppeneinstellung „Wird veröffentlicht" • Gruppeneinstellung „Genehmigung durch Primäreigentümer erforderlich" • Gruppenposition (Einstellung „In Ordner")
Besitzer der Verteilerliste	Gruppenanzeigename	• Gruppenanzeigename • E-Mail-Adresse der Gruppe • Gruppenbeschreibung • Gruppenhinweise • Gruppeneinstellung „Verwaltet von" • Gruppeneinstellung „Wird veröffentlicht" • Gruppeneinstellung „Genehmigung durch Primäreigentümer erforderlich" • Gruppenposition (Einstellung „In Ordner")
Besitzer des Exchange-Ressourcenpostfachs	Postfach-Anzeigename	• Postfach-Anzeigename • Postfachtyp • E-Mail-Adresse • Postfachspeicher oder Datenbankposition • Postfachbeschreibung • Postfachposition (Einstellung „In Ordner")

RESSOURCENTYP	RESSOURCENNAME	RESSOURCENDETAILS
Besitzer des Exchange-Kontakts	Kontakt-Anzeigename	• Anzeigename • Vorname • Nachname • E-Mail-Adresse • Telefonnummer • Firma • Position (Einstellung „In Ordner“)
Besitzer des Computers	Computername	• Computername • Computer-DNS-Name • Computerbeschreibung • Betriebssystem • Position (Einstellung „In Ordner“)
Eigentümer der Ressource (Standard)	Name des verwalteten Objekts	• Name des verwalteten Objekts • Beschreibung des verwalteten Objekts • Position des verwalteten Objekts (Einstellung „In Ordner“)

Freigabe des Zugriffs auf dass Berechtigungsprofil

Standardmäßig geht die Berechtigung zum Anzeigen des Berechtigungsprofils an den ActiveRoles-Admin, das Administrationskonto oder die Gruppe, das/die bei der Installation von Quest One ActiveRoles definiert wird. Andere Benutzer oder Gruppen können auch zum Anzeigen des Berechtigungsprofils zugelassen werden. Für diesen Zweck wird eine dedizierte Zugriffsvorlage bereitgestellt, sodass Sie die Nutzung des Befehls **Berechtigungsprofil** durch definierte Benutzer oder Benutzergruppen zulassen können.

Damit bestimmte Benutzer oder Gruppen das Berechtigungsprofil von Benutzern in einem bestimmten Container sehen können (z. B. eine Organisationseinheit oder eine verwaltete Einheit), müssen Sie die Zugriffsvorlage wie folgt anwenden.

Freigeben des Zugriffs auf das Berechtigungsprofil

1. Klicken Sie in der Quest One ActiveRoles-Konsole mit der rechten Maustaste auf den Container und dann auf **Kontrolle delegieren**, um das Fenster **Quest One ActiveRoles-Sicherheit** anzuzeigen.
2. Klicken Sie im Fenster **Quest One ActiveRoles-Sicherheit** auf **Hinzufügen**, um den Assistenten zum Delegieren der Kontrolle zu starten.
3. Klicken Sie im Assistenten auf **Weiter**.
4. Klicken Sie auf der Seite **Benutzer oder Gruppen** auf **Hinzufügen**, und wählen Sie die gewünschten Benutzer/Gruppen aus.
5. Klicken Sie auf **Weiter**.
6. Erweitern Sie auf der Seite **Zugriffsvorlagen** den Ordner **Active Directory | Erweitert**, und wählen Sie die Option **Benutzer - Berechtigungsprofil anzeigen (erweitertes Recht)** aus.
7. Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen im Assistenten; übernehmen Sie bei diesem Vorgang die Standardeinstellungen.

Nach Abschluss dieser Schritte sind die in Schritt 4 ausgewählten Benutzer und Gruppen zum Anzeigen des Berechtigungsprofils der Benutzer im in Schritt 1 gewählten Container und in dessen Unter-Containern berechtigt.

13

Papierkorb

- Beschreibung der Papierkorbfunktion
- Suchen und Auflisten gelöschter Objekte
- Wiederherstellen eines gelöschten Objekts
- Delegieren von Vorgängen an gelöschten Objekten
- Anwenden von Richtlinien- oder Arbeitsablaufregeln

Beschreibung der Papierkorbfunktion

Quest One ActiveRoles setzt zur Erleichterung der Wiederherstellung gelöschter Objekte auf den Papierkorb von Active Directory, eine in Microsoft Windows Server 2008 R2 eingeführte Funktion der Domain-Dienste von Active Directory, auf. Bei eingeschaltetem Papierkorb ist es unter Quest One ActiveRoles ganz einfach, versehentlich ausgeloste Löschvorgange rückgängig zu machen, wodurch der Aufwand an Zeit und Kosten sowie das Ausmaß der mit der Wiederherstellung gelöschter Objekte in Active Directory verbundenen Belastungen für den Benutzer verringert werden können.

Durch den Einsatz von Quest One ActiveRoles in Verbindung mit dem Papierkorb von Active Directory lassen sich die durch das versehentliche Loschen von Verzeichnisdaten bedingten Ausfallzeiten des Verzeichnisdienstes minimieren. Der Papierkorb schafft die Möglichkeit zur Wiederherstellung gelöschter Objekte ohne Zuhilfenahme von Sicherungskopien oder den Neustart der Domain-Controller. Zudem beschleunigt eine von Quest One ActiveRoles bereitgestellte Arbeitsoberflache das Auffinden und die Wiederherstellung gelöschter Objekte aus dem Papierkorb. Die von Quest One ActiveRoles gebotenen anpassungs- und leistungsfähigen Verfahren zur Delegation von Verwaltungsaufgaben sowie zur Durchsetzung der Richtlinien und Freigaben und zur Nachverfolgung von Änderungen gewährleisten eine lückenlose Überwachung des Wiederherstellungsvorgangs.

Um Löschvorgänge rückgängig zu machen, stützt sich Quest One ActiveRoles auf die Möglichkeit des Active Directory-Papierkorbs, alle Attribute einschließlich der mit Verknüpfungen verbundenen Attribute der gelöschten Objekte beizubehalten. Hierdurch ist es möglich, gelöschte Objekte in den Status zurückzuversetzen, in dem sie sich unmittelbar vor dem Löschvorgang befunden haben. So erhalten zum Beispiel wiederhergestellte Benutzerkonten alle Gruppenmitgliedschaften zurück, die sie vor dem Löschvorgang besessen haben.

Quest One ActiveRoles kann zur Wiederherstellung gelöschter Objekte in jeder verwalteten Domain mit eingeschaltetem Active Directory-Papierkorb verwendet werden. Dies erfordert die Gesamtstruktur-Funktionsebene von Windows Server 2008 R2, sodass alle Gesamtstruktur-Domänencontroller Windows Server 2008 R2 ausführen müssen. In einer Gesamtstruktur, die diese Voraussetzungen erfüllt, kann ein Administrator den Papierkorb mit Hilfe des Active Directory-Moduls für Windows PowerShell in Windows Server 2008 R2 aktivieren. Weitere Informationen über den Active Directory-Papierkorb finden Sie unter Neues in den AD DS: Active Directory-Papierkorb (http://go.microsoft.com/fwlink/?LinkId=141392).

Suchen und Auflisten gelöschter Objekte

Wenn der Active Directory-Papierkorb in einer verwalteten Domäne aktiviert ist, ermöglicht Quest One ActiveRoles den Zugriff auf den Container **Gelöschte Objekte**, der die gelöschten Objekte aus dieser Domäne enthält. In dem Baum der Programmsteuerung von Quest One ActiveRoles wird der Container auf derselben Ebene angezeigt wie die Domain selbst, nämlich unter dem **Active Directory**-Knoten. Wenn für mehrere verwaltete Domänen der Active Directory-Papierkorb aktiviert ist, dann wird ein separater Container für jede Domäne angezeigt. Um die Container voneinander unterscheiden zu können, enthält der Name des Containers den Domänennamen (zum Beispiel **MeineDomäne.MeinComputer.com - Gelöschte Objekte**).

Die Suche-Seiten in der Programmsteuerung von Quest One ActiveRoles erleichtern das Auffinden gelöschter Objekte, indem sie die Verwendung sehr spezifischer Anfragen auf der Grundlage beliebiger Objekteigenschaften ermöglichen. Es ist außerdem möglich, eine Liste der gelöschten Objekte, die sich zum Zeitpunkt des Löschvorgangs in einer bestimmten Organisationseinheit oder verwalteten Einheit befunden haben, zu untersuchen und zu durchsuchen.

Suchen nach dem Container „Gelöschte Objekte"

Die Quest One ActiveRoles-Programmsteuerung bietet die Suchkategorie **Gelöschte Objekte** im Dialogfeld **Suchen**, sie ist zur Durchführung der Suche in dem Container mit den **Gelöschten Objekten** einer jeden verwalteten Domain mit eingeschaltetem Active Directory-Papierkorb gedacht.

Gehen Sie folgendermaßen vor, um nach dem Container „Gelöschte Objekte" zu suchen:

1. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Container **Gelöschte Objekte** und klicken Sie dann auf **Suchen**
2. Führen Sie einen der nachfolgend aufgeführten Schritte aus:
   - Geben Sie im Feld **Name** oder **Beschreibung** den Namen bzw. die Beschreibung oder einen Teil des Namens oder der Beschreibung des zu suchenden Objekts ein.

     *Bei der namensbezogenen Suche verwendet Quest One ActiveRoles den Suchalgorithmus der nicht eindeutigen Auflösung des Namens (ANR), um Objekte ausfindig zu machen, bei denen nicht nur der Name sondern auch einige weitere Eigenschaften der von Ihnen in dem Feld **Name** angegebenen Zeichenfolge entsprechen. Die für ANR verwendeten Eigenschaften umfassen den Namen, den Vornamen, den Nachnamen, den Anzeigenamen und den Anmeldenamen.*

   - Klicken Sie auf die Schaltfläche neben dem Feld **Gelöscht aus** und wählen Sie das Objekt aus, bei dem es sich um das übergeordnete Objekt des zu suchenden, gelöschten Objekts handelt.

     *Mit der Suchoption **Gelöscht aus** können Sie nach untergeordneten Objekten suchen, die aus einem bestimmten Containerobjekt gelöscht wurden.*

   - Verwenden Sie die Registerkarte **Erweitert**, um eine Abfrage auf der Grundlage von anderen Eigenschaften des zu suchenden gelöschten Objekts zu erstellen. Anweisungen finden Sie im Abschnitt Verfahren zum Verwenden von erweiterten Optionen für die Suche und Verfahren zum Anlegen einer benutzerdefinierten Suche weiter oben in diesem Dokument.
3. Klicken Sie zum Starten der Suche auf **Jetzt suchen**.

Nach Abschluss der Suche wird im Dialogfeld **Suchen** eine Liste der mit den Suchkriterien übereinstimmenden gelöschten Objekte angezeigt.

Wenn Sie auf ein Objekt in der Liste der Suchergebnisse doppelklicken, werden die Eigenschaftenseiten für dieses Objekt angezeigt. Wenn Sie mit der rechten Maustaste auf ein Objekt klicken, werden im Kontextmenü alle Aktionen angezeigt, die Sie an diesem Objekt durchführen können.

Suchen nach Objekten, die aus einer bestimmten Organisationseinheit oder verwalteten Einheit gelöscht wurden

Um eine Liste der Objekte anzuzeigen und zu durchsuchen, die aus einer bestimmten Organisationseinheit oder verwalteten Einheit gelöscht wurden, können Sie den Befehl **Gelöschte Objekte anzeigen oder wiederherstellen** verwenden. Der Befehl öffnet ein Dialogfeld, in dem die gelöschten Objekte aufgeführt sind, die der entsprechenden Organisationseinheit oder verwalteten Einheit zum Zeitpunkt des Löschvorgangs direkt untergeordnet waren. Das Dialogfeld **Gelöschte Objekte anzeigen oder wiederherstellen** kann für die Suche nach gelöschten Objekten verwendet werden, deren Name mit einer bestimmten Suchzeichenkette übereinstimmt. Es bietet eine flexible Übereinstimmung, da es die mehrdeutige Namensauflösung (Ambiguous Name Resolution, ANR) unterstützt.

Gehen Sie folgendermaßen vor, um nach Objekten zu suchen, die aus einer bestimmten Organisationseinheit oder verwalteten Einheit gelöscht wurden:

1. Klicken Sie mit der rechten Maustaste auf die Organisationseinheit oder verwaltete Einheit und klicken Sie dann auf **Gelöschte Objekte anzeigen oder wiederherstellen**.
2. Geben Sie im Feld **Suchen nach** die Suchzeichenkette ein, die Sie verwenden möchten.
3. Klicken Sie zum Starten der Suche auf **Jetzt suchen**.

Wenn die Suche abgeschlossen ist, ist die Liste im Dialogfeld auf die gelöschten Objekte beschränkt, deren Name, Vorname, Nachname, Anzeigename, Anmeldename oder jegliche andere für ANR verwendete Eigenschaft mit der angegebenen Suchzeichenkette beginnt. Um die Suchergebnisse zu löschen und alle gelöschten Objekte anzuzeigen, klicken Sie auf die Schaltfläche **Suche löschen**.

Der Befehl **Gelöschte Objekte anzeigen oder wiederherstellen** ist auch für Domänen- und Containerobjekte verfügbar. Somit können Sie auch nach gelöschten Objekten suchen, die zum Zeitpunkt des Löschvorgangs einer bestimmten Domäne oder einem bestimmten Container direkt untergeordnet waren.

Wiederherstellen eines gelöschten Objekts

Für die Wiederherstellung von gelöschten Objekten können Sie den Befehl **Wiederherstellen** verwenden, der in folgenden Elementen verfügbar ist:

- Das Dialogfeld **Gelöschte Objekte anzeigen oder wiederherstellen**
- In einer Liste der Suchergebnisse, die mit Hilfe der Suchkategorie **Gelöschte Objekte** im Dialogfeld **Suchen** vorbereitet wird
- In einer Liste der Objekte, die sich im Container **Gelöschte Objekte** befinden; diese Liste wird im Bereich „Details" angezeigt, wenn Sie den Container **Gelöschte Objekte** in der Konsolenstruktur auswählen

In der Programmsteuerung von Quest One ActiveRoles findet sich der Befehl in dem Kontextmenu, das mit einem Rechtsklick auf das jeweilige Objekt aufgerufen werden kann.

Gehen Sie folgendermaßen vor, um ein gelöschtes Objekt wiederherzustellen:

1. Klicken Sie im Dialogfeld **Gelöschte Objekte anzeigen oder wiederherstellen** auf das gelöschte Objekt und klicken Sie dann auf die Schaltfläche **Wiederherstellen**.

   – ODER –

   Klicken Sie in einer Liste der Suchergebnisse, die mit Hilfe der Suchkategorie **Gelöschte Objekte** vorbereitet wurde, oder in einer Liste der Objekte, die sich im Container **Gelöschte Objekte** befinden, mit der rechten Maustaste auf das gelöschte Objekt und dann auf **Wiederherstellen**.

2. Überprüfen und ändern Sie bei Bedarf die Einstellungen im Dialogfeld **Objekt wiederherstellen** und klicken Sie dann auf **OK**, um den Wiederherstellungsvorgang zu starten.

Im Dialogfeld **Objekt wiederherstellen** werden Sie aufgefordert, festzulegen, ob gelöschte untergeordnete Objekte des gelöschten Objekts ebenfalls wiederhergestellt werden sollen. Das Kontrollkästchen **Untergeordnete Objekte wiederherstellen** ist standardmäßig aktiviert. Dies gewährleistet, dass der auf ein gelöschtes Containerobjekt angewandte Befehl **Wiederherstellen** den gesamten Inhalt des Containers wiederherstellt.

Betrachten Sie zur Veranschaulichung das Beispiel, in dem ein Administrator versehentlich die Organisationseinheit mit dem Namen „Sales_Department", die eine Reihe von Benutzerkonten für das Vertriebspersonal enthält, gemeinsam mit einer anderen Organisationseinheit mit der Bezeichnung „Admins", die ihrerseits ein Benutzerkonto für einen administrativen Assistenten enthält, löscht. Bei Anwendung des Befehls **Wiederherstellen** auf die Organisationseinheit „Sales_Department" mit der Option zur Wiederherstellung von untergeordneten Objekten führt Quest One ActiveRoles die folgenden Schritte aus:

1. Wiederherstellung der Organisationseinheit „Sales_Department"
2. Wiederherstellung aller gelöschten Benutzerkonten, die der Organisationseinheit „Sales_Department" direkt untergeordnet waren
3. Wiederherstellung der Organisationseinheit „Admins" in der Organisationseinheit „Sales_Department"
4. Wiederherstellung aller gelöschten Benutzerkonten, die der Organisationseinheit „Admins" direkt untergeordnet waren

Wenn Sie das Kontrollkästchen **Untergeordnete Objekte wiederherstellen** deaktivieren, führt Quest One ActiveRoles nur den ersten Schritt durch, sodass die wiederhergestellte Organisationseinheit „Sales_Department" leer ist.

Stellen Sie bei der Wiederherstellung eines gelöschten Objekts sicher, dass sein übergeordnetes Objekt nicht gelöscht wird. Das übergeordnete Objekt können Sie durch Anzeige der Eigenschaften des gelöschten Objekts ermitteln: Der kanonische Name des übergeordneten Objekts, dem die Bezeichnung „gelöscht aus:" voransteht, wird neben dem Namen des gelöschten Objekts auf der Registerkarte **Allgemein** im Dialogfeld **Eigenschaften** angezeigt. Wenn das übergeordnete Objekt gelöscht ist, müssen Sie es wiederherstellen, bevor Sie dessen untergeordnete Objekte wiederherstellen, da gelöschte Objekte in einem aktiven übergeordneten Objekt wiederhergestellt werden müssen.

Delegieren von Vorgängen an gelöschten Objekten

Das auf den Zugriffsvorlagen von Quest One ActiveRoles beruhende Delegationsmodell kann vollständig auf die dem Löschen von Objekten eigenen Verwaltungsvorgange angewendet werden. Eine neue Zugriffsvorlage mit der Bezeichnung **All Objects - View or Restore Deleted Objects** erleichtert die Delegation der folgenden Vorgänge an ausgewählten Benutzer:

- Anzeigen gelöschter Active Directory-Objekte
- Wiederherstellen eines gelöschten Active Directory-Objekts

Bei Anwendung auf den Container **Gelöschte Objekte** verleiht die Zugriffsvorlage den delegierten Benutzern das Recht, jedes beliebige gelöschte Objekt anzuzeigen und wiederherzustellen. Bei Anwendung der Zugriffsvorlage auf eine Organisationseinheit oder eine verwaltete Einheit erhalten die delegierten Benutzer das Recht, nur die gelöschten Objekte anzuzeigen und wiederherzustellen, die sich zum Zeitpunkt des Löschvorgangs in dieser Organisationseinheit oder verwalteten Einheit befunden haben.

Gehen Sie folgendermaßen vor, um den Vorgang der Wiederherstellung gelöschter Objekte zu delegieren:

1. Wählen Sie in der Konsolenstruktur **Configuration | Access Templates | Active Directory**.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf **All Objects – View or Restore Deleted Objects** und klicken Sie dann auf **Verknüpfungen**.

3. Klicken Sie im Dialogfeld **Verknüpfungen** auf **Hinzufügen**
4. Klicken Sie auf der Begrüßungsseite im Assistenten zum Delegieren der Kontrolle auf **Weiter**.
5. Klicken Sie auf der Seite **Objekte** im Assistenten auf **Hinzufügen**; wählen Sie dann den Container aus, in dem Sie den Vorgang der Wiederherstellung von gelöschten Objekten delegieren möchten:
   - Um die Wiederherstellung nur von den gelöschten Objekte zu delegieren, die sich zum Zeitpunkt des Löschvorgangs in einer bestimmten Organisationseinheit oder verwalteten Einheit befunden haben, wählen Sie die Organisationseinheit oder verwaltete Einheit aus.
   - Um die Wiederherstellung jedes beliebigen gelöschten Objekts in einer bestimmten verwalteten Domäne zu delegieren, wählen Sie entweder das Objekt, das diese Domäne angibt, oder den Container **Gelöschte Objekte** für diese Domäne aus.
   - Um die Wiederherstellung jedes beliebigen gelöschten Objekts in jeder beliebigen verwalteten Domäne zu delegieren, wählen Sie den Container **Active Directory** aus.
6. Befolgen Sie die Anweisungen des Assistenten, um den Assistenten zum Delegieren der Kontrolle abzuschließen.
7. Klicken Sie auf **OK**, um das Dialogfeld **Verknüpfungen** zu schließen.

Obwohl die Delegierung des Vorgangs zur Wiederherstellung gelöschter Objekte in allen verwalteten Domains, Organisationseinheiten (OU) oder verwalteten Einheiten (MU) möglich ist, kann ein gelöschtes Objekt mit Hilfe von Quest One ActiveRoles nur dann wiederhergestellt werden, wenn es zu einer verwalteten Domain mit eingeschaltetem Active Directory-Papierkorb gehört. Anweisungen bezüglich der Aktivierung des Papierkorbs finden Sie unter „Schrittweise Anleitung zum Active Directory-Papierkorb" in der Dokumentation zu Windows Server 2008 R2 von Microsoft.

Anwenden von Richtlinien- oder Arbeitsablaufregeln

Zusätzlich zur Delegierung von Verwaltungsaufgaben bietet Quest One ActiveRoles die Möglichkeit zur Einrichtung einer richtliniengestutzten Überwachung des Wiederherstellungsvorgangs für gelöschte Objekte. Richtlinienregeln können verwendet werden, um zusätzliche Überprüfung oder benutzerdefinierte skriptbasierte Vorgänge bei der Wiederherstellung von gelöschten Objekten durchzuführen. Es können Arbeitsablaufregeln angewandt werden, die die Genehmigung für den Wiederherstellungsvorgang oder eine Benachrichtigung per E-Mail über den Abschluss des Wiederherstellungsvorgangs erfordern.

Die Richtlinien- oder Arbeitsablaufregeln für die Kontrolle des Wiederherstellungsvorgangs oder für die sonstige Verwaltung gelöschter Objekte kann in folgenden Elementen definiert werden:

- Der **Active Directory**-Knoten in der Quest One ActiveRoles-Programmsteuerung - Die auf diese Weise festgelegten Regeln gelten für alle gelöschten Objekte in allen verwalteten Domains, für die der Papierkorb eingeschaltet ist.
- Der Knoten, der eine Domain oder den Container mit den **Gelöschten Objekten** dieser Domain in der Programmsteuerung von Quest One ActiveRoles abbildet - Diese Regeln gelten lediglich für alle gelöschten Objekte dieser einen Domain.
- Eine Organisations- (OU) oder verwaltete Einheit (MU), in denen sich das Objekt zum Zeitpunkt der Löschung befindet. Auch wenn das gelöschte Objekt nicht langer Teil der OU oder MU ist, wird der ehemalige Netzwerkstandort des Objektes von Quest One ActiveRoles weiterhin berücksichtigt, sodass die auf diesen Standort angewendeten Regeln auch nach der Löschung noch für das Objekt gelten.

Ein Administrator kann zum Beispiel einen Arbeitsablauf so konfigurieren, dass eine Genehmigung für die Wiederherstellung eines jeden Benutzerkontos erforderlich ist, das aus einer bestimmten Organisationseinheit gelöscht wurde. Die Arbeitsablaufdefinition enthält in diesem Fall eine entsprechende Genehmigungsregel und gibt diese Organisationseinheit als den Zielcontainer in den Arbeitsablauf-Startbedingungen an.

Richtlinienregeln werden per Konfiguration und Anwendung von Richtlinienobjekten definiert.

So wenden Sie ein Richtlinienobjekt auf den Container „Gelöschte Objekte" an:

1. Klicken Sie mit der rechten Maustaste auf den Container **Gelöschte Objekte** und klicken Sie dann auf **Richtlinie erzwingen**.
2. Klicken Sie in dem Dialogfeld **Quest One ActiveRoles Richtlinien** auf **Hinzufügen**.
3. Aktivieren Sie im Dialogfeld **Richtlinienobjekte auswählen** das Kontrollkästchen neben dem Richtlinienobjekt, das Sie anwenden möchten, und klicken Sie dann auf **OK**.
4. Klicken Sie auf **OK**, um das Dialogfeld **Quest One ActiveRoles-Richtlinie** zu schließen.

Weitere Informationen und Anweisungen bezüglich der Konfiguration und Anwendung von Richtlinienobjekten finden Sie im Abschnitt Anwenden von Richtlinienobjekten weiter oben in diesem Dokument.

Arbeitsablaufregeln werden durch Konfiguration von Arbeitsablaufdefinitionen und Festlegung der entsprechenden Arbeitsablauf-Startbedingungen definiert.

Gehen Sie folgendermaßen vor, um einen Arbeitsablauf auf den Container „Gelöschte Objekte" anzuwenden:

1. Wählen Sie in der Konsolenstruktur den Arbeitsablauf aus, den Sie anwenden möchten.

   *Um einen Arbeitsablauf auszuwählen, erweitern Sie **Configuration | Policies | Workflow** und klicken Sie dann auf das Arbeitsablaufdefinitionsobjekt unter **Workflow** in der Konsolenstruktur.*

2. Klicken Sie in dem Angabenfenster die Schaltfläche **Auswahlmöglichkeiten und Startvoraussetzungen für den Arbeitsablauf** über dem Arbeitsablaufdiagramm an und anschließend auf **Konfigurieren**

   *Darauf wird die Seite **Auswahlmöglichkeiten und Startvoraussetzungen für den Arbeitsablauf** angezeigt.*

3. Klicken Sie auf **Vorgang auswählen**, wählen Sie die Option **Wiederherstellen** und klicken Sie dann auf **Fertig stellen**.

   Hierdurch wird der Arbeitsablauf bei einer Anforderung zur Wiederherstellung eines gelöschten Objekts des angegebenen Typs gestartet.

4. Klicken Sie auf **Hinzufügen** unter **Initiatorbedingungen**.
5. Klicken Sie auf der Seite **Initiatorbedingung hinzufügen** auf **Durchsuchen** und wählen Sie dann den Container **Gelöschte Objekte**.

   *Sie müssen einen anderen Container als **Gelöschte Objekte** auswählen. Wenn Sie dies tun, startet der Arbeitsablauf nur bei der Wiederherstellung eines Objekts, das aus dem von Ihnen ausgewählten Container gelöscht wurde.*

6. Schließen Sie die Konfiguration der Arbeitsablauf-Startbedingungen ab.

Ausführlichere Informationen über Arbeitsabläufe finden Sie im Kapitel Arbeitsabläufe weiter oben in diesem Dokument.

14

AD LDS-Datenverwaltung

- Registrieren einer AD LDS-Instanz
- Verwalten von AD LDS-Objekten
- Konfigurieren von Quest One ActiveRoles für AD LDS

Eine Quest One ActiveRoles-Lizenz ermöglicht normalerweise nicht die AD LDS-Datenverwaltung. Damit Quest One ActiveRoles AD LDS-Datenverwaltungsaufgaben durchführen kann, ist eine separate Lizenz erforderlich.

Registrieren einer AD LDS-Instanz

Quest One ActiveRoles bietet die Möglichkeit, Verzeichnisdaten in Microsoft Active Directory Lightweight Directory Services (AD LDS), einem unabhängigen Modus von Active Directory, zuvor bekannt unter der Bezeichnung „Active Directory Application Mode" (ADAM), zu verwalten.

Eine laufende Kopie des AD LDS Verzeichnisdiensts wird als eine Dienstinstanz (oder einfach *Instanz*) bezeichnet. Um Quest One ActiveRoles für die Verwaltung von Daten zu verwenden, die vom AD LDS Verzeichnisdienst gehostet werden, müssen Sie zunächst die Instanz registrieren, in der sich die zu verwaltenden Daten befinden.

Wenn eine Instanz registriert wurde, können die Quest One ActiveRoles Client-Schnittstellen – Konsole, Web-Interface und ADSI Provider – verwendet werden, um die Verzeichnisdaten in den in der Instanz gefundenen Anwendungs- und Konfigurationspartitionen aufzurufen, anzuzeigen und zu ändern. Die bei Quest One ActiveRoles registrierten Instanzen werden als *verwaltete AD LDS-Instanzen* bezeichnet.

Gehen Sie folgendermaßen vor, um eine AD LDS-Instanz bei Quest One ActiveRoles zu registrieren:

1. Öffnen Sie die Quest One ActiveRoles-Konsole.
2. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Server configuration**, klicken Sie mit der rechten Maustaste auf **Managed AD LDS Instances (ADAM)** und wählen Sie **Neu | Verwaltete AD LDS-Instanz (ADAM)**, um den Assistenten zum Hinzufügen von verwalteten AD LDS-Instanzen zu starten.
3. Folgen Sie den Anweisungen des Assistenten.
4. Geben Sie auf der Seite **Zu registrierende AD LDS-Instanz** den Servernamen und die Portnummer der AD LDS-Instanz an, die Sie bei Quest One ActiveRoles registrieren möchten.

   Geben Sie unter **Server** den vollqualifizierten DNS-Namen (zum Beispiel server.company.com) des Computers an, auf dem die Instanz ausgeführt wird. Geben Sie unter **LDAP-Anschluss** die Nummer des Lightweight Directory Access Protocol (LDAP) Kommunikationsanschlusses an, der von der Instanz verwendet wird (der Standard-Kommunikationsanschluss für LDAP ist 389). Sie können auch auf **Auswählen** klicken, um die AD LDS-Instanz, die Sie registrieren möchten, zu suchen und auszuwählen.

5. Geben Sie auf der Seite **Quest One ActiveRoles-Anmeldeinformationen** die Anmeldeinformationen an, die Quest One ActiveRoles für den Zugriff auf die Instanz verwenden wird.

   Wenn Sie möchten, dass jeder Verwaltungsdienst im Sicherheitskontext seines eigenen Dienstkonto die Verbindung zur Instanz herstellt, dann klicken Sie auf **Die Dienstkontoinformationen, die der Verwaltungsdienst zur Anmeldung verwendet**. Bei Auswahl dieser Option können verschiedene Verwaltungsdienste unterschiedliche Zugriffsebenen auf die Instanz haben (das Dienstkonto eines Dienstes kann administrative Zugriffsrechte auf die Instanz haben, während das Dienstkonto eines anderen Dienstes nicht über diese Rechte verfügt). Folglich kann der Wechsel von einem Verwaltungsdienst zum anderen dazu führen, dass Quest One ActiveRoles den Zugriff auf die Instanz verliert.

   Wenn Sie möchten, dass jeder Verwaltungsdienst mit Hilfe desselben Benutzerkontos eine Verbindung zur Instanz aufbaut, dann klicken Sie auf **Die unten angegebenen Windows Benutzerkontoinformationen** und geben Sie den Benutzernamen, das Kennwort und den Domänennamen ein. Auf diese Weise geben Sie ein so genanntes *Vorrangiges Konto* an, wodurch die Zugriffsrechte von Quest One ActiveRoles auf die Instanz von den Zugriffsrechten dieses Benutzerkontos bestimmt werden (anstatt von den Zugriffsrechten des Dienstkontos des Verwaltungsdienstes).

6. Klicken Sie auf der Abschlussseite auf **Fertig stellen**, um den Registrierungsvorgang zu starten.

Das von Ihnen in Schritt 5 angegebene vorrangige Konto muss über die vollständige administrative Kontrolle über diese Instanz verfügen. D.h. es muss ein Mitglied der Administratorengruppe in der Konfigurationsverzeichnispartition der Instanz sein. Wenn Sie sich dazu entschließen, kein vorrangiges Konto anzugeben, dann müssen Sie sicherstellen, dass das Dienstkonto jeder Ihrer Verwaltungsdienste dieser Anforderung entspricht. Verwenden Sie das ADAM ADSI Edit Snap-in, um das vorrangige Konto oder das Dienstkonto zur Administratorengruppe in der Konfigurationsverzeichnispartition hinzuzufügen, bevor Sie die Instanz bei Quest One ActiveRoles registrieren.

Nach der Registrierung einer AD LDS (ADAM) Instanz können Sie ihre Registrierungseinstellungen anzeigen oder ändern, indem Sie den Befehl **Eigenschaften** für das Objekt ausführen, das diese Instanz im Container **Managed AD LDS Instances (ADAM)** repräsentiert. Dann können Sie Änderungen an den in Schritt 5 oben ausgewählten Optionen vornehmen.

Wenn Sie eine AD LDS (ADAM) Instanz nicht mehr mit Quest One ActiveRoles verwalten möchten, können Sie die Registrierung der Instanz aufheben, indem Sie den Befehl **Löschen** für das Objekt ausführen, das diese Instanz im Container **Managed AD LDS Instances (ADAM)** repräsentiert. Durch die Aufhebung der Registrierung einer Instanz werden nur die Registrierungsinformationen von Quest One ActiveRoles entfernt. Es werden keine Änderungen an den von dieser Instanz gehosteten Verzeichnisdaten vorgenommen.

Verwalten von AD LDS-Objekten

Die in den verwalteten AD LDS-Instanzen gefundenen Anwendungs- und Konfigurationspartitionen werden in einem Container der obersten Ebene zusammengefasst, was das Auffinden der AD LDS-Daten erleichtert. Jede Partition wird durch einen separaten Container (Knoten) dargestellt, sodass Sie die Partitionsstruktur auf gleiche Weise durchblättern können, wie Sie dies für eine Active Directory-Domäne tun.

Die Quest One ActiveRoles-Konsole unterstützt eine Vielzahl von administrativen Vorgängen an AD LDS-Benutzern, Gruppen und anderen Objekten. Sie können Verzeichnisobjekte wie etwa Benutzer, Gruppen und Organisationseinheiten in den verwalteten AD LDS-Instanzen auf gleiche Weise erstellen, anzeigen, ändern und löschen, wie Sie dies für Verzeichnisobjekte in Active Directory-Domänen tun.

Gehen Sie folgendermaßen vor, um die Verzeichnisstruktur zu durchzublättern und um ADLDS-Objekte zu verwalten:

1. Doppelklicken Sie in der Konsolenstruktur unter dem Stammverzeichnis der Konsolenstruktur auf den Container **AD LDS (ADAM)**.
2. Doppelklicken Sie in der Konsolenstruktur unter **AD LDS (ADAM)** auf ein Verzeichnispartitionsobjekt, um dessen Container der obersten Ebene anzuzeigen.
3. Doppelklicken Sie in der Konsolenstruktur auf einen Container der obersten Ebene, um die nächste Objektebene in diesem Container anzuzeigen.
4. Führen Sie einen der nachfolgend aufgeführten Schritte aus:
   - Um die nächst tiefere Verzweigung der Verzeichnisstruktur anzuzeigen, doppelklicken Sie auf die nächst tiefere Containerebene in der Konsolenstruktur.
   - Um ein Verzeichnisobjekt auf der aktuellen Verzeichnisebene zu verwalten, klicken Sie mit der rechten Maustaste auf das Verzeichnisobjekt im Bereich „Details" und verwenden Sie die Befehle im Kontextmenü.

Im Container **AD LDS (ADAM)** ist jede Verzeichnispartition durch eine Bezeichnung gekennzeichnet, die sich aus dem Namen der Partition, dem DNS-Namen des Computers, auf dem die AD LDS-Instanz ausgeführt wird, die die Partition hostet, und der Nummer des von der Instanz verwendeten LDAP-Anschlusses zusammensetzt.

Normalerweise zeigt die Konsole nur die Anwendungsverzeichnispartitionen an. Um die Konfigurations- oder Schemapartition anzuzeigen, wechseln Sie in den Rohansichtsmodus: Wählen Sie **Ansicht | Modus**, klicken Sie auf **Rohmodus** und dann auf **OK**.

Sie können nur die Datenverwaltungsaufgaben ausführen, denen Sie in Quest One ActiveRoles zugeordnet sind. Daher werden nur die Befehle, die Sie verwenden dürfen, und die Objekte, die Sie anzeigen oder ändern dürfen, angezeigt.

Zusätzlich zur Zugriffskontrolle ermöglicht Quest One ActiveRoles die Richtlinienumsetzung für Verzeichnisdaten. Richtlinien können den Zugriff auf bestimmte Teile der Verzeichnisobjekte einschränken, was zur Folge hat, dass Dateneinträge auf eine Auswahl von Optionen beschränkt wird, dass Daten automatisch generiert werden und es keine Möglichkeit zur Änderung der Daten gibt oder dass die Eingabe von Daten erforderlich ist. Die Konsole bietet eine visuelle Markierung der Dateneinträge, die durch Richtlinien kontrolliert werden: Die Bezeichnungen derartiger Dateneinträge sind in den Dialogfeldern unterstrichen, sodass der Benutzer Richtlinieneinschränkungen untersuchen kann, indem er auf eine Bezeichnung klickt.

Hinzufügen eines AD LDS-Benutzers zum Verzeichnis

Um die Erstellung von Benutzern in AD LDS zu ermöglichen, muss der Administrator zunächst die optionalen Definitionen der von AD LDS bereitgestellten Benutzerobjektklassen importieren. Diese Definitionen sind in importfähigen .ldf-Dateien (ms-User.ldf, ms-InetOrgPerson.ldf, ms-UserProxy.ldf), die sich auf dem Computer befinden, der die AD LDS-Instanz ausführt. Alternativ können die Softwareentwickler das AD LDS-Schema um ihre benutzerdefinierten Definitionen von ADLDS-Benutzerobjektklassen erweitern. Details bezüglich der Erweiterung des AD LDS-Schemas finden Sie in der Dokumentation von Microsoft, die im Lieferumfang von AD LDS enthalten ist.

Gehen Sie folgendermaßen vor, um einen AD LDS-Benutzer zum Verzeichnis hinzuzufügen:

1. Klicken Sie in der Konsolenstruktur unter **AD LDS (ADAM)** mit der rechten Maustaste auf den Container, zu dem Sie den Benutzer hinzufügen möchten, und wählen Sie dann **Neu|Benutzer**, um den Assistenten zu starten, der Sie bei der Durchführung der Benutzererstellung unterstützt.
2. Befolgen Sie die Anweisungen des Assistenten, um die Werte für die Benutzereigenschaften festzulegen.
3. Wenn Sie Werte für zusätzliche Eigenschaften festlegen möchten (solche, für die der Assistent keine Dateneingaben vorsieht), klicken Sie auf der letzten Seite des Assistenten auf **Attribute bearbeiten**.
4. Nachdem Sie die Einstellungen für alle zusätzlichen Eigenschaften für den neuen Benutzer festgelegt haben, klicken Sie auf der letzten Seite des Assistenten auf **Fertig stellen**.

Standardmäßig wird ein AD LDS-Benutzer aktiviert, wenn der Benutzer erstellt wird. Wenn Sie jedoch einem neuen AD LDS-Benutzer ein falsches Kennwort zuordnen oder das Kennwort leer lassen, kann das neu erstellte AD LDS-Benutzerkonto deaktiviert werden. Eine unter Windows Server 2003 ausgeführte AD LDS-Instanz erzwingt also automatisch die Anwendung aller vorhandenen lokalen oder Domänen-Kennwortrichtlinien. Wenn Sie einen neuen AD LDS-Benutzer erstellen und diesem Benutzer ein Kennwort zuweisen, das nicht den Anforderungen der gültigen Kennwortrichtlinie entspricht, wird das neu erstellte Benutzerkonto deaktiviert. Bevor Sie das Benutzerkonto aktivieren können, müssen Sie ein Kennwort für das Konto festlegen, das den Einschränkungen der Kennwortrichtlinie entspricht. Die Anweisungen bezüglich der Festlegung des Kennworts für einen AD LDS-Benutzer und der Aktivierung eines AD LDS-Benutzers sind weiter unten in diesem Abschnitt aufgeführt.

Hinzufügen einer AD LDS-Gruppe zum Verzeichnis

AD LDS bietet Standardgruppen, die sich im Container **Rollen** jeder Verzeichnispartition in AD LDS befinden. Sie können bei Bedarf zusätzliche AD LDS-Gruppen erstellen. Neue Gruppen können in jedem beliebigen Container erstellt werden.

Gehen Sie folgendermaßen vor, um eine AD LDS-Gruppe zum Verzeichnis hinzuzufügen:

1. Klicken Sie in der Konsolenstruktur unter **AD LDS (ADAM)** mit der rechten Maustaste auf den Container, zu dem Sie die Gruppe hinzufügen möchten, und wählen Sie dann **Neu|Gruppe**, um den Assistenten zu starten, der Sie bei der Durchführung der Gruppenerstellung unterstützt.
2. Befolgen Sie die Anweisungen des Assistenten, um die Werte für die Gruppeneigenschaften festzulegen.
3. Wenn Sie Werte für zusätzliche Eigenschaften festlegen möchten (solche, für die der Assistent keine Dateneingaben vorsieht), klicken Sie auf der letzten Seite des Assistenten auf **Attribute bearbeiten**.
4. Nachdem Sie die Einstellungen für alle zusätzlichen Eigenschaften für die neue Gruppe festgelegt haben, klicken Sie auf der letzten Seite des Assistenten auf **Fertig stellen**.

Sie können sowohl AD LDS-Benutzer als auch Windows-Benutzer zu den von Ihnen erstellten ADLDS-Gruppen hinzufügen. Anweisungen finden Sie im folgenden Unterabschnitt.

Hinzufügen oder Entfernen von Mitgliedern zu bzw. aus einer AD LDS-Gruppe

Beim Hinzufügen von Mitgliedern zu einer AD LDS-Gruppe können Sie Sicherheitsprinzipals hinzufügen, die sich in AD LDS-Instanzen oder in Active Directory-Domänen befinden. Beispiele für Sicherheitsprinzipals sind AD LDS-Benutzer und Active Directory-Domänenbenutzer und gruppen.

1. Gehen Sie folgendermaßen vor, um Mitglieder zu einer AD LDS-Gruppe hinzuzufügen bzw. aus ihr zu entfernen:
2. Wählen Sie in der Konsolenstruktur unter **AD LDS (ADAM)** den Container aus, in dem sich die Gruppe befindet.
3. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf die Gruppe und klicken Sie dann auf **Eigenschaften**.
4. Klicken Sie auf der Registerkarte **Mitglieder** im Dialogfeld **Eigenschaften** auf **Hinzufügen**
5. Verwenden Sie das Dialogfeld **Objekte auswählen**, um die Sicherheitsprinzipals auszuwählen, die Sie zur Gruppe hinzufügen möchten. Klicken Sie abschließend auf **OK**.
6. Wählen Sie auf der Registerkarte **Mitglieder** die Gruppenmitglieder aus, die Sie aus der Gruppe entfernen möchten, und klicken Sie dann auf **Entfernen**.
7. Nachdem Sie die gewünschten Änderungen an der Gruppe vorgenommen haben, klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** zu schließen.

Wenn Sie das Dialogfeld „Objekte auswählen" für die Suche eines Sicherheitsprinzipals verwenden, müssen Sie zunächst die AD LDS-Verzeichnispartition oder die Active Directory-Domäne angeben, in der sich der Sicherheitsprinzipal befindet: Klicken Sie auf **Durchsuchen** und wählen Sie die entsprechende Partition oder Domäne aus.

Sie können nur Sicherheitsprinzipals auswählen, die sich in verwalteten AD LDS-Instanzen oder Active Directory-Domänen befinden; d. h., Sie können Sicherheitsprinzipals nur aus den Instanzen und Domänen auswählen, die bei Quest One ActiveRoles registriert sind.

Deaktivieren oder Aktivieren eines ADLDS-Benutzerkontos

Sie können das Konto eines AD LDS-Benutzers deaktivieren, um zu verhindern, dass sich der Benutzer bei der AD LDS-Instanz Replikation von Verwaltungsverlaufsdaten mit diesem Konto anmeldet.

Gehen Sie folgendermaßen vor, um ein AD LDS-Benutzerkonto zu deaktivieren bzw. zu aktivieren:

1. Wählen Sie in der Konsolenstruktur unter **AD LDS (ADAM)** den Container aus, in dem sich das Benutzerkonto befindet.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf das Benutzerkonto und führen Sie einen der folgenden Schritte durch, um den Status des Kontos zu ändern:
   - Wenn das Benutzerkonto aktiviert ist, klicken Sie auf **Konto deaktivieren**.
   - Wenn das Benutzerkonto deaktiviert ist, klicken Sie auf **Konto aktivieren**.

Wenn der AD LDS-Benutzer, dessen Konto Sie deaktivieren möchten, aktuell bei der AD LDS-Instanz angemeldet ist, muss sich dieser Benutzer abmelden, damit die neuen Einstellungen übernommen werden.

Normalerweise wird ein AD LDS-Benutzer aktiviert, wenn der Benutzer erstellt wird. Wenn das Kennwort eines neuen AD LDS-Benutzer jedoch nicht den Anforderungen der gültigen Kennwortrichtlinie entspricht, wird das neu erstellte Benutzerkonto deaktiviert. Bevor Sie das Benutzerkonto aktivieren können, müssen Sie ein Kennwort für das Konto festlegen, das den Einschränkungen der Kennwortrichtlinie entspricht. Anweisungen finden Sie im folgenden Unterabschnitt.

Festlegen oder Ändern des Kennworts eines ADLDS-Benutzers

Jedem AD LDS Sicherheitsprinzipal wie etwa einem AD LDS-Benutzer muss ein Konto und Kennwort zugeordnet werden, das AD LDS für die Authentifizierung verwendet. Sie können die Quest One ActiveRoles-Konsole verwenden, um das Kennwort eines AD LDS-Benutzers festzulegen oder zu ändern.

Gehen Sie folgendermaßen vor, um das Kennwort eines AD LDS-Benutzers festzulegen oder zu ändern:

1. Wählen Sie in der Konsolenstruktur unter **AD LDS (ADAM)** den Container aus, der das Benutzerkonto des AD LDS-Benutzers enthält, für den Sie das Kennwort festlegen oder ändern möchten.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf das Benutzerkonto und klicken Sie dann auf **Kennwort zurücksetzen**.
3. Geben Sie im Dialogfeld **Kennwort zurücksetzen** ein Kennwort für den Benutzer in das Feld **Neues Kennwort** ein und geben Sie das Kennwort dann erneut in das Feld **Kennwortbestätigung** ein oder klicken Sie auf die Schaltfläche neben **Neues Kennwort**, um ein Kennwort zu generieren.
4. Klicken Sie auf **OK**, um das Dialogfeld **Kennwort zurücksetzen** zu schließen.

Der AD LDS-Benutzer, für den Sie das Kennwort festlegen oder ändern, muss dieses neue Kennwort beim nächsten Mal verwenden, wenn er sich bei AD LDS anmeldet.

Standardmäßig erzwingt eine unter Windows Server 2003 oder höher ausgeführte AD LDS-Instanz automatisch die Anwendung aller vorhandenen lokalen oder Domänen-Kennwortrichtlinien. Wenn Sie ein Kennwort für einen AD LDS-Benutzer festlegen, das nicht den Anforderungen der gültigen Kennwortrichtlinie entspricht, gibt Quest One ActiveRoles einen Fehler aus.

Hinzufügen einer Organisationseinheit zum Verzeichnis

Um Ihre AD LDS-Benutzer und Gruppen zu organisieren, können Sie Benutzer und Gruppen in Organisationseinheiten zusammenfassen. In AD LDS sowie in Active Directory oder anderen auf dem Lightweight Directory Access Protocol (LDAP) basierenden Verzeichnissen sind Organisationseinheiten die am häufigsten verwendete Methode, um Benutzer und Gruppen zu organisieren. Um eine Organisationseinheit in AD LDS zu erstellen, können Sie die Quest One ActiveRoles-Konsole wie nachfolgend beschrieben nutzen.

Gehen Sie folgendermaßen vor, um eine Organisationseinheit zum Verzeichnis hinzuzufügen:

1. Klicken Sie in der Konsolenstruktur unter **AD LDS (ADAM)** mit der rechten Maustaste auf den Container, zu dem Sie die Organisationseinheit hinzufügen möchten, und wählen Sie **Neu | Organisationseinheit**.
2. Geben Sie einen Namen für die neue Organisationseinheit ein, klicken Sie auf **Weiter** und klicken Sie dann auf **Fertig stellen**.

Standardmäßig können Organisationseinheiten nur unter den Objektklassen Organisationseinheit (ou=), Land/Region (c=), Organisation (o=) oder Domänen-DNS (dc=) hinzugefügt werden. Sie können zum Beispiel eine Organisationseinheit zu o=Unternehmen,c=US aber nicht zu cn=Anwendung,o=Unternehmen,c=US hinzufügen. Die Schemadefinition der Objektklasse „Organisationseinheit" kann jedoch geändert werden, um andere Einteilungen zu ermöglichen.

Sie können neue AD LDS-Benutzer und Gruppen in einer AD LDS-Organisationseinheit erstellen. Wenden Sie dazu den Befehl **Neu | Benutzer** oder **Neu | Gruppe** wie weiter oben in diesem Abschnitt beschrieben auf die Organisationseinheit an.

Sie können einen vorhandenen AD LDS-Benutzer oder eine vorhandene AD LDS-Gruppe in eine Organisationseinheit verschieben. Wenden Sie dazu den Befehl **Verschieben** auf diesen Benutzer oder diese Gruppe in der Quest One ActiveRoles-Konsole an oder verwenden Sie die Drag & Drop-Funktion der Konsole.

Hinzufügen eines AD LDS (ADAM)-Proxyobjekts (Benutzerproxy)

AD LDS-Proxyobjekte werden in besonderen Fällen verwendet, in denen eine Anwendung eine einfache LDAP-Bindung an AD LDS durchführen kann, aber die Anwendung den AD LDS-Benutzer immer noch mit einem Sicherheitsprinzipal (Benutzerkonto) in Active Directory verknüpfen muss. Ein Prozess, durch den AD LDS eine Bindungsanforderung von einer Anwendung akzeptieren und diese Bindungsanforderung auf der Grundlage des Inhalts eines Proxyobjekts an Active Directory umleiten kann, wird als *Bindungsumleitung* bezeichnet.

Die Bindungsumleitung tritt ein, wenn eine Bindung zu AD LDS mit Hilfe eines Proxyobjekts (Benutzerproxy) versucht wird. Ein Proxyobjekt ist ein Objekt in AD LDS, das ein Benutzerkonto in Active Directory angibt. Jedes Proxyobjekt in AD LDS enthält die Sicherheits-ID (SID) eines Benutzers in Active Directory. Wenn eine Anwendung versucht, eine Bindung zu einem Proxyobjekt herzustellen, nimmt AD LDS die SID, die im Proxyobjekt gespeichert ist, zusammen mit dem Kennwort, das zum Zeitpunkt der Bindung angegeben wurde, und liefert Active Directory die SID und das Kennwort zu Authentifizierungszwecken.

Ein Proxyobjekt in AD LDS stellt ein Active Directory-Benutzerkonto dar; es kann vergrößert werden, um zusätzliche Daten zu speichern, die in Zusammenhang mit dem anwendungsspezifischen Benutzerkonto stehen. Durch die Bindungsumleitung können Anwendungen den Identitätsspeicher von Active Directory nutzen und gleichzeitig die Flexibilität der Verwendung von AD LDS als einen Anwendungsdatenspeicher beibehalten.

Gehen Sie folgendermaßen vor, um ein Proxyobjekt zu AD LDS hinzuzufügen:

1. Erweitern Sie in der Konsolenstruktur den Container **AD LDS (ADAM)**.
2. Erweitern Sie in der Konsolenstruktur unter **AD LDS (ADAM)** die Verzeichnispartition, zu der Sie ein Proxyobjekt hinzufügen möchten, und suchen Sie den Container, zu dem Sie das Proxyobjekt hinzufügen möchten.
3. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Container, zu dem Sie das Proxyobjekt hinzufügen möchten, und wählen Sie **Neu | Proxy-Objekt**, um den Assistenten zu starten, der Sie bei der Erstellung eines Proxyobjekts unterstützt.
4. Geben Sie einen Namen für das Proxyobjekt ein. Klicken Sie dann auf **Weiter**.
5. Klicken Sie auf **Auswählen** und wählen Sie das Active Directory-Domänen-Benutzerkonto, das durch das Proxyobjekt angegeben werden soll. Klicken Sie dann auf **Weiter**.
6. Wenn Sie Werte für zusätzliche Eigenschaften festlegen möchten (solche, für die der Assistent keine Dateneingaben vorsieht), klicken Sie auf der letzten Seite des Assistenten auf **Attribute bearbeiten**.
7. Nachdem Sie die Einstellungen für alle zusätzlichen Eigenschaften für das neue Objekt festgelegt haben, klicken Sie auf der letzten Seite des Assistenten auf **Fertig stellen**.

Sie können ein vorhandenes Proxyobjekt untersuchen, indem Sie den Befehl **Eigenschaften** für dieses Objekt ausführen. Das Dialogfeld **Eigenschaften** ermöglicht Ihnen, das von dem Proxyobjekt angegebene Benutzerkonto anzuzeigen. Aufgrund einer Einschränkung von AD LDS kann diese Einstellung jedoch nicht für ein vorhandenes Proxyobjekt geändert werden. Sie können ein Active Directory-Domänen-Benutzerkonto nur während der Erstellung des Proxyobjekts auswählen. Nach der Erstellung eines Proxyobjekts kann diese Einstellung nicht mehr geändert werden.

Wenn Sie ein Proxyobjekt erstellen, können Sie ein Benutzerkonto aus jeder beliebigen Domäne auswählen, die bei Quest One ActiveRoles registriert ist, vorausgesetzt, dass der Domäne von dem Computer vertraut wird, auf dem die AD LDS-Instanz ausgeführt wird.

Ein Proxyobjekt für einen Domänenbenutzer kann nicht in einer AD LDS-Verzeichnispartition erstellt werden, die bereits ein fremdes Prinzipalobjekt (FPO) oder ein Proxyobjekt für denselben Domänenbenutzer enthält.

Für ein bestimmtes Benutzerkonto in Active Directory können Sie eine Liste der Proxyobjekte anzeigen, die das Benutzerkonto in AD LDS angeben: Rufen Sie im Dialogfeld **Eigenschaften** für das Benutzerkonto die Registerkarte **Objekt** auf und klicken Sie dann auf **AD LDS-Proxy-Objekte**.

Konfigurieren von Quest One ActiveRoles für AD LDS

Nachfolgend sind die die AD LDS-Datenverwaltungsspezifischen und mit der Konfiguration von Quest One ActiveRoles verbundenen Aufgaben aufgeführt:

- **Bereitstellen von regelbasierten administrativen Ansichten.** Sie können verwaltete Einheiten in Quest One ActiveRoles so konfigurieren, dass sie virtuelle Zusammenstellungen von Verzeichnisobjekten von AD LDS, Active Directory oder beiden für die Verteilung von administrativen Verantwortlichkeiten und für die Erzwingung von Geschäftsregeln und -richtlinien darstellen.
- **Implementieren einer rollenbasierten Delegation.** Sie können Quest One ActiveRoles-Zugriffsvorlagen anwenden, um die Kontrolle über AD LDS-Daten zu delegieren. Dies erfolgt auf gleiche Weise, wie Sie dies für die in Active Directory-Domänen gespeicherten Verzeichnisdaten tun.

- **Richtlinienbasierte Kontrolle und automatische Bereitstellung von Verzeichnisdaten.** Sie können Quest One ActiveRoles-Richtlinienobjekte anwenden, um richtlinienbasierte Kontrollen einzurichten und die automatische Bereitstellung von AD LDS-Daten durchzuführen. Dies erfolgt auf gleiche Weise, wie Sie dies für die in Active Directory-Domänen gespeicherten Verzeichnisdaten tun.

Dies erfolgt auf gleiche Weise, wie Sie dies für die in Active Directory-Domänen gespeicherten Verzeichnisdaten tun.

In diesem Abschnitt wird jede dieser Aufgaben eingehend beschrieben

Mit Hilfe der Quest One ActiveRoles-Konsole können Sie verwaltete Einheiten in Quest One ActiveRoles so konfigurieren, dass sie virtuelle Zusammenstellungen von Verzeichnisobjekten von AD LDS, Active Directory oder beiden für die Verteilung von administrativen Verantwortlichkeiten und für die Erzwingung von Geschäftsregeln darstellen. Bei Konfiguration verwalteter Einheiten, sodass diese Verzeichnisobjekte von jedem Speicherort (ganz gleich, ob es AD LDS oder Active Directory ist) aufnehmen können, bietet Quest One ActiveRoles die Möglichkeit, eine rollenbasierte Delegation und eine richtlinienbasierte administrative Kontrolle von Verzeichnisdaten ohne Berücksichtigung der Verzeichnisgrenzen zu implementieren, wo dies erforderlich ist.

Gehen Sie wie nachfolgend beschrieben vor, um eine vorhandene verwaltete Einheit so zu konfigurieren, dass sie AD LDS-Objekte wie etwa AD LDS-Benutzer, Gruppen oder Organisationseinheiten enthalten kann. Ausführlichere Anweisungen bezüglich der Erstellung und Verwaltung von verwalteten Einheiten finden Sie im Abschnitt „Regelbasierte administrative Ansichten" weiter oben in diesem Dokument.

Gehen Sie folgendermaßen vor, um eine vorhandene verwaltete Einheit so zu konfigurieren, dass sie von einer Abfrage ausgegebene AD LDS-Objekte aufnimmt:

1. Klicken Sie mit der rechten Maustaste auf die verwaltete Einheit und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie auf der Registerkarte **Mitgliedschaftsregeln** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Mitgliedschaftsregeltyp** auf **Nach Abfrage einschließen** und klicken Sie dann auf **OK**.
4. Verwenden Sie das Dialogfeld **Mitgliedschaftsregel erstellen**, um die Abfrage einzurichten:
   a) Klicken Sie in der Liste **Suchen** auf **Benutzerdefinierte Suche**.
   b) Klicken Sie auf **Durchsuchen** neben dem Feld **In**.
   c) Erweitern Sie im Dialogfeld **Container suchen** den Container **AD LDS (ADAM)**, erweitern Sie dann die AD LDS-Verzeichnispartition, die die Objekte enthält, die die Abfrage ausgeben soll, und wählen Sie den Container, in dem sich diese Objekte befinden. Klicken Sie dann auf **OK**.
   d) Klicken Sie auf die Schaltfläche **Feld** und wählen Sie die Objekttypen, die die Abfrage ausgeben soll, sowie die Objekteigenschaft, die Sie abfragen möchten.
   e) Klicken Sie unter **Bedingung** auf die Bedingung für Ihre Abfrage und geben Sie dann unter **Wert** einen Eigenschaftswert ein, damit Ihre Abfrage die Objekte ausgibt, die die Objekteigenschaft haben, die mit dem von Ihnen angegebenen Bedingungswert-Paar übereinstimmen.
   f) Klicken Sie auf die Schaltfläche **Hinzufügen**, um diese Abfragebedingung zur Abfrage hinzuzufügen.

g) Wiederholen Sie optional die Schritte d) bis f), um ihre Abfrage durch das Hinzufügen weiterer Bedingungen zu präzisieren. Wenn die Abfrage die Objekte ausgeben soll, die allen angegebenen Bedingungen entsprechen, klicken Sie auf **UND**. Wenn die Abfrage die Objekte ausgeben soll, die einer beliebigen der angegebenen Bedingungen entsprechen, klicken Sie auf **ODER**.

h) Klicken Sie optional auf **Regelvorschau**, um eine Liste der Objekte anzuzeigen, die Ihre Abfrage ausgibt. Beachten Sie, dass die Abfrageergebnisse abhängig vom aktuellen Status der Daten im Verzeichnis variieren können. Die verwaltete Einheit wird die Abfrage immer dann, wenn Änderungen an den Verzeichnisdaten durchgeführt wurden, automatisch erneut anwenden, um zu gewährleisten, dass die Mitgliedschaftsliste der verwalteten Einheit aktuell und richtig ist.

i) Klicken Sie auf die Schaltfläche **Regel hinzufügen**.

5. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** für die verwaltete Einheit zu schließen.

Sie können auch Mitgliedschaftsregeln von anderen Kategorien als „Nach Abfrage einschließen" konfigurieren, um AD LDS-Objekte aus einer verwalteten Einheit aufzunehmen bzw. auszuschließen. Wählen Sie hierzu die entsprechende Kategorie im Dialogfeld **Mitgliedschaftsregeltyp** aus. Weitere Schritte für die Konfiguration einer Mitgliedschaftsregel sind allesamt an die Verwendung des Dialogfelds **Mitgliedschaftsregel erstellen** für die Konfiguration einer bestimmten Abfrage oder an die Verwendung des Dialogfelds „Objekte auswählen" zum Auswählen eines bestimmten Objekts gebunden.

Anzeigen oder Festlegen von Berechtigungen für ADLDS-Objekte

Mit Hilfe der Quest One ActiveRoles-Konsole können Sie Quest One ActiveRoles-Zugriffsvorlagen anwenden, um die Kontrolle über AD LDS-Daten zu delegieren. Dies erfolgt auf gleiche Weise, wie Sie dies für die in Active Directory-Domänen gespeicherten Verzeichnisdaten tun. Durch die Anwendung von Zugriffsvorlagen auf Benutzer oder Gruppen (Trustees) von AD LDS-Objekten und Containern können Sie die entsprechende Zugriffsebene auf die in AD LDS gespeicherten Verzeichnisdaten für die Trustees einrichten und sie somit zur Durchführung einer genau festgelegten Reihe von Aktivitäten befugen, die mit der ADLDS-Datenverwaltung in Verbindung stehen.

Quest One ActiveRoles bietet eine umfassende Palette an vorkonfigurierten Zugriffsvorlagen, um die Delegation von AD LDS-Datenverwaltungsaufgaben zu erleichtern. Eine Liste der AD LDS-spezifischen Zugriffsvorlagen finden Sie im Dokument *Sofort verwendbare Zugriffsvorlagen*, das Teil der Quest One ActiveRoles-Dokumentation ist. Diese Zugriffsvorlagen befinden sich im Container**Configuration/ Access Templates/AD LDS (ADAM)** in der Quest One ActiveRoles-Konsole.

Gehen Sie wie nachfolgend beschrieben vor, um zu überprüfen, welche Zugriffsvorlagen auf ein bestimmtes AD LDS-Objekt wie etwa ein AD LDS-Benutzer, eine Gruppe, eine Organisationseinheit, ein Container oder die gesamte Verzeichnispartition angewandt wurden und um Zugriffsvorlagen hinzuzufügen oder zu entfernen, um die Ebene des Zugriffs zu ändern, den die Trustees auf dieses Objekt haben.

Ausführlichere Anweisungen bezüglich der Erstellung, Konfiguration und Anwendung von Zugriffsvorlagen finden Sie im Abschnitt „Rollenbasierte Administration" weiter oben in diesem Dokument.

Gehen Sie folgendermaßen vor, um die Liste der Zugriffsvorlagen für ein AD LDS-Objekt anzuzeigen oder zu ändern:

1. Wählen Sie in der Konsolenstruktur unter **AD LDS (ADAM)** den Container aus, der das Objekt enthält, für das Sie die Liste der Zugriffsvorlagen anzeigen oder ändern möchten.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf das Objekt und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf der Registerkarte **Verwaltung** im Dialogfeld **Eigenschaften** auf **Sicherheit**.
4. Zeigen Sie im Dialogfeld **Quest One ActiveRoles-Sicherheit** die Liste der Zugriffsvorlagen an, die auf das AD LDS-Objekt angewandt wurden, oder ändern Sie die Liste wie folgt:
   - Um eine zusätzliche Zugriffsvorlage auf das Objekt anzuwenden, klicken Sie auf **Hinzufügen** und befolgen Sie die Anweisungen des Assistenten zum Zuweisen der Objektverwaltung.
   - Um von einer Zugriffsvorlage für das Objekt angegebene Berechtigungen zu entfernen, wählen Sie die Zugriffsvorlage in der Liste aus und klicken Sie dann auf **Entfernen**.
5. Klicken Sie auf **OK**, um das Dialogfeld **Quest One ActiveRoles-Sicherheit** zu schließen.
6. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** für das AD LDS-Objekt zu schließen.

Im Assistent für die Kontrolldelegierung können Sie die Benutzer oder Gruppen (Trustees) auswählen, die die Berechtigungen erhalten sollen, und wählen dann eine oder mehrere Zugriffsvorlagen aus dem Container **Access Templates/AD LDS (ADAM)** aus, um die Berechtigungen zu definieren. Als Folge haben die von Ihnen ausgewählten Trustees die Berechtigungen, die von den Zugriffsvorlagen für das AD LDS-Objekt definiert sind. Die Trustees können die Berechtigung lediglich innerhalb von Quest One ActiveRoles ausführen, da Quest One ActiveRoles keine Berechtigungseinstellungen an AD LDS überträgt.

Im Dialogfeld **Quest One ActiveRoles-Sicherheit** kann eine Zugriffsvorlage nur entfernt werden, wenn sie auf das Objekt angewandt wird, das Sie ausgewählt haben (statt auf einen Container, in dem das Objekt gespeichert ist). Um die Zugriffsvorlagen anzuzeigen, die aus der aktuellen Auswahl entfernt werden können, deaktivieren Sie das Kontrollkästchen **Vererbung anzeigen**.

Anstatt eine Zugriffsvorlage im Dialogfeld **Quest One ActiveRoles-Sicherheit** zu entfernen, können Sie die Zugriffsvorlage auswählen und dann auf **Deaktivieren** klicken, um die Berechtigungen für die Objekte zurückzunehmen, die von der Zugriffsvorlage definiert sind. Auf diese Weise können Sie die Auswirkungen einer Zugriffsvorlage vermeiden, und zwar unabhängig davon, ob die Zugriffsvorlage auf das Objekt selbst oder auf einen Container, in dem sich das Objekt befindet, angewandt wird. Sie können diesen Vorgang rückgängig machen, indem Sie die Zugriffsvorlage auswählen und dann auf **Aktivieren** klicken.

Anzeigen oder Festlegen von Richtlinien für ADLDS-Objekte

Mit Hilfe der Quest One ActiveRoles-Konsole können Sie Quest One ActiveRoles-Richtlinienobjekte anwenden, um richtlinienbasierte Kontrollen einzurichten und die automatische Bereitstellung von AD LDS-Daten durchzuführen. Dies erfolgt auf gleiche Weise, wie Sie dies für die in Active Directory-Domänen gespeicherten Verzeichnisdaten tun. Durch die Bereitstellung der Möglichkeit, betriebliche Richtlinien streng durchzusetzen und einen nicht kontrollierten Zugriff auf sensible, in AD LDS gespeicherte Informationen zu unterbinden, gewährleistet die Hilfe von Quest One ActiveRoles die Sicherheit Ihrer unternehmenskritischen Daten. Richtlinienobjekte können so konfiguriert werden, dass sie eine Vielzahl von Richtlinien wie auf AD LDS angewandt festlegen. Hierzu zählen unter anderem die Überprüfung von Datenformaten, die regelbasierte, automatische Bereitstellung bestimmter Datenbereiche in AD LDS und skriptbasierte, benutzerdefinierte Vorgänge an AD LDS-Daten.

Gehen Sie wie nachfolgend beschrieben vor, um eine Liste der Richtlinienobjekte anzuzeigen oder zu ändern, die auf ein bestimmtes AD LDS-Objekt wie etwa einen AD LDS-Benutzer, eine Gruppe, eine Organisationseinheit, einen Container oder die gesamte Verzeichnispartition angewandt wurden. Ausführlichere Anweisungen bezüglich der Erstellung, Konfiguration und Anwendung von Richtlinienobjekten finden Sie im Abschnitt „Regelbasierte automatische Bereitstellung und Deprovisionierung" weiter oben in diesem Dokument.

Gehen Sie folgendermaßen vor, um die Liste der Richtlinienobjekte für ein AD LDS-Objekt anzuzeigen oder zu ändern:

1. Wählen Sie in der Konsolenstruktur unter **AD LDS (ADAM)** den Container aus, der das Objekt enthält, für das Sie die Liste der Richtlinienobjekte anzeigen oder ändern möchten.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf das Objekt und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf der Registerkarte **Verwaltung** im Dialogfeld **Eigenschaften** auf **Richtlinie**.
4. Zeigen Sie im Dialogfeld **Quest One ActiveRoles-Richtlinie** die Liste der Richtlinienobjekte an, die Auswirkungen auf das AD LDS-Objekt haben, oder ändern Sie die Liste wie folgt:
   - Um ein weiteres Richtlinienobjekt auf das AD LDS-Objekt anzuwenden, klicken Sie auf **Hinzufügen**, wählen dann das anzuwendende Richtlinienobjekt aus und klicken Sie dann auf **OK**.
   - Um die Auswirkung eines Richtlinienobjekts auf das AD LDS-Objekt aufzuheben, wählen Sie das Richtlinienobjekt in der Liste aus und klicken Sie dann auf **Entfernen**. Aktivieren Sie alternativ dazu das Kontrollkästchen **Gesperrt** neben dem Namen des Richtlinienobjekts.
5. Klicken Sie auf **OK**, um das Dialogfeld **Quest One ActiveRoles-Richtlinie** zu schließen.
6. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** für das AD LDS-Objekt zu schließen.

Im Dialogfeld **Quest One ActiveRoles-Richtlinie** kann ein Richtlinienobjekt nur entfernt werden, wenn es auf das AD LDS-Objekt angewandt wird, das Sie ausgewählt haben (anstelle auf einen Container, in dem sich das AD LDS-Objekt befindet). Um die Richtlinienobjekte anzuzeigen, die aus der aktuellen Auswahl entfernt werden können, klicken Sie auf **Erweitert** und deaktivieren Sie dann das Kontrollkästchen **Vererbung anzeigen**.

Anstatt ein Richtlinienobjekt im Dialogfeld **Quest One ActiveRoles-Serverrichtlinie** zu entfernen, können Sie das Kontrollkästchen **Gesperrt** in dem Listeneintrag für das Richtlinienobjekt aktivieren, um die Auswirkungen des Richtlinienobjekts auf das AD LDS-Objekt aufzuheben. Auf diese Weise können Sie die Auswirkungen eines Richtlinienobjekts vermeiden, und zwar unabhängig davon, ob das Richtlinienobjekt auf das AD LDS-Objekt selbst oder auf einen Container, in dem sich das Objekt befindet, angewandt wird. Wenn Sie ein Richtlinienobjekt für ein bestimmtes AD LDS-Objekt sperren, haben die von diesem Richtlinienobjekt definierten Richtlinieneinstellungen keine Auswirkungen mehr auf das AD LDS-Objekt. Sie können diese Vorgang durch Deaktivieren des Kontrollkästchens **Gesperrt** rückgängig machen.

15

Verwaltung der Einrichtungseinstellungen von Quest One ActiveRoles

- Einleitung
- Herstellen einer Verbindung zum Verwaltungsdienst
- Hinzufügen und Entfernen verwalteter Domänen
- Konfigurieren von nicht verwalteten Domänen
- Konfigurieren der Replikation
- Verwenden der Datenbankspiegelung
- Erstellen und Verwenden virtueller Attribute
- Untersuchen von Client-Sitzungen
- Überwachen der Leistung
- Anpassen der Konsole
- Änderung des Administratorenkontos für ActiveRoles
- Das Programm zur Verbesserung der Software

Einleitung

In diesem Kapitel werden die folgenden Verwaltungsaktivitäten untersucht:

- Herstellen einer Verbindung zum Verwaltungsdienst
- Die Anmeldung von Domains mittels Quest One ActiveRoles
- Konfigurieren der Replikation des Verwaltungsdienstes
- Erstellen und Verwenden virtueller Attribute
- Untersuchen von Client-Sitzungen und Überwachen der Leistung
- Die individuelle Einrichtung der Quest One ActiveRoles-Programmsteuerung

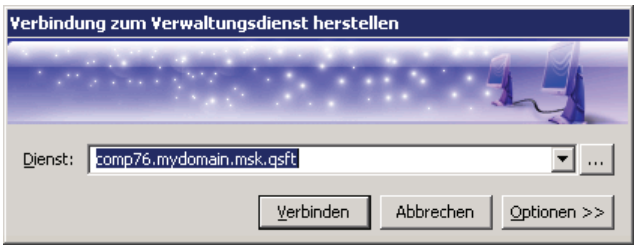
Um die Konfiguration des Verwaltungsdienstes zu administrieren, benötigen Sie geeignete Berechtigungen. Es ist ausreichend, ein Mitglied im Konto der Administratoren von ActiveRoles zu sein. Das Konto der Administratoren von ActiveRoles wird bei der Installation des Verwaltungsdienstes angegeben. Es entspricht standardmäßig der Administratorengruppe auf dem Computer, auf dem der Verwaltungsdienst ausgeführt wird.

Die Autorisierung, die Konfiguration des Verwaltungsdienstes zu ändern, kann delegiert werden. Wenden Sie dazu die Zugriffsvorlage **Manage Configuration** auf den Container **Server Configuration** an.

Herstellen einer Verbindung zum Verwaltungsdienst

Um mithilfe der Programmsteuerung von Quest One ActiveRoles einen bestimmten Verwaltungsdienst einzurichten, muss der Verwaltungsdienst, zu dem die Verbindung hergestellt werden soll, manuell angeben werden. Andernfalls wählt die Konsole automatisch den Verwaltungsdienst aus.

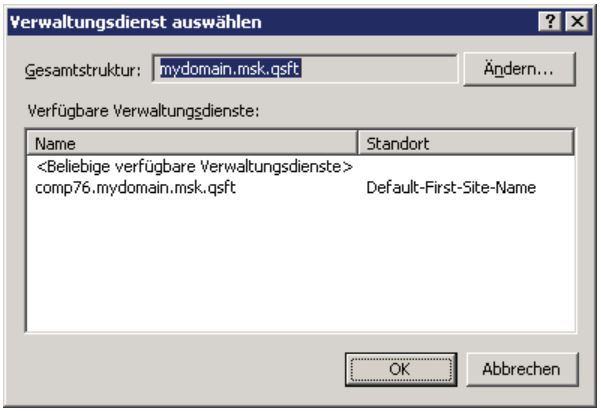
Sie können das Dialogfeld **Verbindung zum Verwaltungsdienst herstellen** verwenden, um den entsprechenden Verwaltungsdienst manuell auszuwählen. Klicken Sie, um dieses Dialogfeld aufzurufen, im Baum der Programmsteuerung mit der rechten Maustaste auf **Quest One ActiveRoles** und anschließend mit links auf **Verbinden**. Das Dialogfeld entspricht der folgenden Abbildung.



Geben Sie im Fenster **Dienst** den Namen des Computers ein, auf dem der Verwaltungsdienst ausgeführt wird, zu dem eine Verbindung hergestellt werden soll, oder wählen Sie den Namen aus. Klicken Sie dann auf **Verbinden**. Das Feld **Dienst** bietet eine Liste der Namen, die für vorige Verbindungssitzungen angegeben wurden. Standardmäßig wird der zuletzt ausgewählte Name angezeigt.

Um einen nicht in der Liste aufgeführten Verwaltungsdienst auszuwählen, klicken Sie auf die Schaltfläche **Wählen** neben dem Feld **Dienst**:

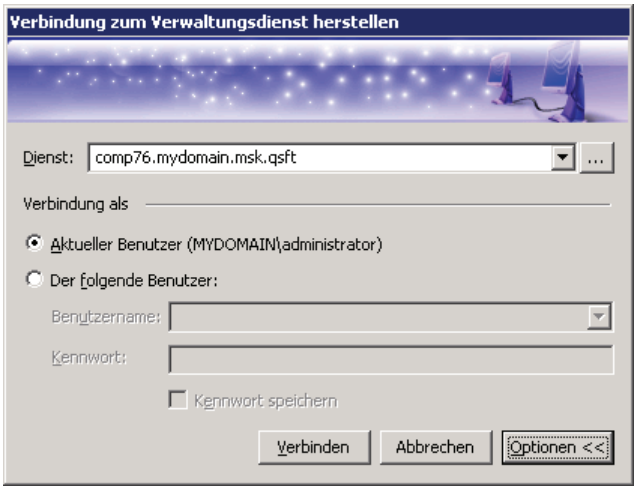
Hierdurch wird das Dialogfeld **Verwaltungsdienst auswählen** angezeigt, das in der folgenden Abbildung dargestellt ist.



Im Dialogfeld **Verwaltungsdienst auswählen** werden die Verwaltungsdienste aufgelistet, die in der angegebenen Gesamtstruktur verfügbar sind. Sie können eine andere Gesamtstruktur durch Anklicken von **Ändern** auswählen. Die Listenelemente sind nach Priorität sortiert. Dabei werden die Seite und die Auslastung des jeweiligen Dienstes beachtet (weniger stark ausgelastete Verwaltungsdienste werden in der Liste ganz oben angezeigt). Um einen bestimmten Dienst zum Dialogfeld **Verbindung zum Verwaltungsdienst herstellen** hinzuzufügen, klicken Sie auf den Dienst und klicken Sie dann auf **OK**.

Wenn Sie eine Verbindung zu einem bestimmten Dienst aufgebaut haben, versucht die Konsole, bei jedem weiteren Start automatisch eine Verbindung zu diesem Dienst aufzubauen. Wenn Sie die Option **<Beliebige verfügbare Verwaltungsdienste>** ausgewählt haben, versucht die Konsole, eine Verbindung zum nächsten, am wenigsten ausgelasteten Dienst in der angegebenen Gesamtstruktur aufzubauen, wobei die Dienste bevorzugt werden, die zur selben Replikationsgruppe wie der Dienst gehören, mit der die Konsole bei der letzten Sitzung verbunden war.

Standardmäßig baut die Konsole die Verbindung zum Verwaltungsdienst im Sicherheitskontext Ihres Anmeldekontos auf (d.h. das Benutzerkonto, mit dem Sie sich angemeldet haben). Das bedeutet, dass Sie die Konsole nur verwenden können, um die Aufgaben auszuführen, die an Ihr Benutzerkonto delegiert wurden. Sie haben die Option, eine Verbindung mit Hilfe eines anderen Kontos aufzubauen, um den Umfang der zulässigen Aufgaben zu erweitern. Klicken Sie auf **Optionen**, um das Dialogfeld **Verbindung zum Verwaltungsdienst herstellen** wie in der folgenden Abbildung gezeigt zu erweitern.



Klicken Sie auf **Der folgende Benutzer** und geben Sie dann Benutzeranmeldenamen und das Kennwort des Kontos an, das für die Verbindung verwendet werden soll. Durch Aktivieren des Kontrollkästchens **Kennwort speichern** verwendet die Konsole automatisch den angegebenen Benutzernamen und das Kennwort bei zukünftigen Verbindungssitzungen. Ansonsten fordert Sie die Konsole bei einem weiteren Start zur Eingabe eines Kennworts auf.

Verfahren zum Herstellen einer Verbindung zum Verwaltungsdienst

Nach jedem Aufruf der Programmsteuerung von Quest One ActiveRoles wird der entsprechende Verwaltungsdienst automatisch ausgewählt und eine Verbindung zu ihm hergestellt. Sie können sich aber auch jederzeit mit einem Verwaltungsdienst Ihrer Wahl verbinden.

Gehen Sie folgendermaßen vor, um den Verwaltungsdienst auszuwählen, zu dem eine Verbindung hergestellt werden soll:

1. Klicken Sie im Baum der Programmsteuerung mit der rechten Maustaste auf **Quest One ActiveRoles** und dann mit links auf **Verbinden**.
2. Geben Sie im Fenster **Dienst** den Namen des Computers ein, auf dem der Verwaltungsdienst ausgeführt wird, zu dem eine Verbindung hergestellt werden soll, oder wählen Sie den Namen aus. Klicken Sie dann auf die Schaltfläche **Verbinden**.

- Wenn der gewünschte Verwaltungsdienst nicht in der Liste **Dienst** angezeigt wird, klicken Sie auf die Schaltfläche **Wählen** neben dem Feld **Dienst**. Hierdurch wird eine Liste der Verwaltungsdienste angezeigt, die in der angegebenen Gesamtstruktur verfügbar sind. Sie können eine andere Gesamtstruktur durch Anklicken von **Ändern** auswählen. Um einen bestimmten Dienst zur Liste **Dienst** hinzuzufügen, klicken Sie auf diesen Dienst in der Liste der verfügbaren Verwaltungsdienste und klicken Sie dann auf **OK**.
- Wenn Sie eine Verbindung unter einem anderen Benutzerkonto als Ihrem Anmeldekonto herstellen müssen, klicken Sie auf **Optionen**, um den Bereich **Verbinden als** anzuzeigen, klicken Sie dann auf **Der folgende Benutzer** und geben Sie den Benutzeranmeldenamen und das Kennwort des Kontos ein, die für die Verbindung verwendet werden sollen. Durch Aktivieren des Kontrollkästchens **Kennwort speichern** verwendet die Konsole automatisch den angegebenen Benutzernamen und das Kennwort bei zukünftigen Verbindungssitzungen. Ansonsten fordert Sie die Konsole bei einem weiteren Start zur Eingabe eines Kennworts auf.

Hinzufügen und Entfernen verwalteter Domänen

Bei Quest One ActiveRoles angemeldete Active Directory-Domains werden als *Verwaltete Domains* bezeichnet. Jeder Verwaltungsdienst pflegt eine Liste verwalteter Domänen und speichert diese Liste als Teil der Dienstkonfiguration in der Verwaltungsdatenbank.

In der Programmsteuerung von Quest One ActiveRoles wird der Assistent „Verwaltete Domain hinzufügen" verwendet, um Domains zur Verwaltung anzumelden. Sie können auf folgende Weise auf den Assistenten zugreifen: Klicken Sie auf das Stammverzeichnis der Konsolenstruktur. Klicken Sie dann im Bereich „Details" im Bereich **Domänen** auf **Domäne hinzufügen**.

Der Assistent „Verwaltete Domäne hinzufügen" fordert Sie zur Eingabe der folgenden Informationen auf:

- Der Name der zu registrierenden Domäne.
- Von Quest One ActiveRoles für den Zugriff auf die Domain verwendete Zugangsdaten.

Sie können die standardmäßigen Rechtezuweisungen verwenden (das Dienstkonto des Verwaltungsdienstes) oder den Benutzernamen und das Kennwort eines anderen Kontos (des vorrangigen Kontos) eingeben. In beiden Fällen muss das Konto über ausreichende Rechte in der verwalteten Domäne verfügen. Ausführlichere Angaben dazu finden sich im Abschnitt „Zugriff auf verwaltete Domains" der Kurzanleitung zur Inbetriebnahme von *Quest One ActiveRoles „Erste Schritte*".

Wenn Sie die Option für den Zugriff auf die verwaltete Domäne mit Hilfe der Dienstkontoinformationen auswählen, beachten Sie die folgenden Hinweise: Diese Option gilt für alle Verwaltungsdienste in Ihrer Umgebung. Jeder Verwaltungsdienst in Ihrer Umgebung verwendet für den Zugriff auf die Domäne sein eigenes Dienstkonto. Da verschiedene Dienstkonten verschiedene Ebenen von Zugriffsrechten bezüglich der Domain aufweisen können, kann Quest One ActiveRoles je nachdem, welcher Verwaltungsdienst für die Verwaltung der Domäne verwendet wird, über unterschiedliche Berechtigungen zum Zugriff auf die Domain verfügt. Infolgedessen kann es beim Wechsel zu einem anderen Verwaltungsdienst Änderungen im Verhalten von Quest One ActiveRoles zu Veränderungen kommen.

Nachdem Sie eine verwaltete Domäne hinzugefügt haben, ruft der Verwaltungsdienst die Domäneninformationen ab, z.B. das Active Directory-Schema und die Containerhierarchie. Dieser Prozess wird als *Laden von Domäneninformationen* bezeichnet.

Das Laden der Informationen in den Verwaltungsdienst kann einige Minuten dauern. Nach Abschluss dieses Prozesses steht die Domäne für die Verwaltung zur Verfügung. Wählen Sie in der Konsolenstruktur das Element **Active Directory** aus, und drücken Sie F5, um den Bereich „Details" zu aktualisieren und die neue Domäne anzuzeigen. Um die Verwaltung der Domäne zu starten, wählen Sie sie im Bereich „Details" aus und drücken Sie dann die Eingabetaste. Oder erweitern Sie das Domänenelement in der Konsolenstruktur.

Sie können eine Domäne aus der Liste der verwalteten Domänen entfernen. Nach dem Entfernen können weder die Domain noch die in ihr enthaltenen Objekte weiter mit Quest One ActiveRoles verwaltet werden. Um eine verwaltete Domäne zu entfernen, wählen Sie das Stammverzeichnis der Konsolenstruktur aus und klicken Sie dann auf **Zu verwalteten Domänen** wechseln im Bereich „Details" im Bereich **Domänen**. Hierdurch wird im Bereich „Details" eine Liste der verwalteten Domänen angezeigt. Klicken Sie in der Liste mit der rechten Maustaste auf die zu entfernende Domäne und klicken Sie dann auf **Löschen**.

Verfahren zum Hinzufügen oder Entfernen einer verwalteten Domäne

Das Hinzufügen einer verwalteten Domäne führt zur Erstellung eines Objekts, das die Registrierungsinformationen über die Domäne enthält. Deshalb wird auch von der Anmeldung einer Domain bei Quest One ActiveRoles gesprochen.

So fügen Sie eine verwaltete Domäne hinzu:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Server Configuration**.
2. Klicken Sie unter **Server Configuration** mit der rechten Maustaste auf **Verwaltete Domänen** und wählen Sie **Neu | Verwaltete Domäne**, um den Assistenten zum Hinzufügen einer verwalteten Domäne zu starten.
3. Klicken Sie auf der Seite Willkommen des Assistenten auf **Weiter**.
4. Führen Sie auf der Seite **Domänenauswahl** einen der folgenden Vorgänge aus und klicken Sie dann auf **Weiter**.
   - Geben Sie den Namen der Domäne ein, die Sie hinzufügen möchten.
   - Klicken Sie auf **Durchsuchen** und wählen Sie die Domäne aus der Liste aus.

5. Klicken Sie auf der Seite der **Zugangsdaten für Quest One ActiveRoles** eine dieser Auswahlmöglichkeiten an, um die Angaben festzulegen, die von Quest One ActiveRoles für den Zugriff auf die Domain verwendet werden sollen:
   - **Die Dienstkontoinformationen, die der Verwaltungsdienst zur Anmeldung verwendet**
   - **Die unten angegebenen Windows-Benutzerkontoinformationen**

   Wenn Sie sich für die zweite Möglichkeit entscheiden, müssen Sie den Benutzernamen und das Passwort für das von Quest One ActiveRoles beim Zugriff auf die Domain zu verwendende Benutzerkonto eingeben.
6. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

So entfernen Sie eine verwaltete Domäne:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Server Configuration**.
2. Klicken Sie unter **Server Configuration** auf **Verwaltete Domänen**.
3. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf die Domäne, die Sie entfernen möchten, und klicken Sie dann auf **Löschen**.

- Sie können den Befehl **Eigenschaften** für jedes im Container **Verwaltete Domänen** enthaltene Objekt verwenden, um die Registrierungsinformationen für die entsprechende verwaltete Domäne anzuzeigen oder zu ändern. So können Sie zum Beispiel die Anmeldeinformationen ändern, die für den Zugriff auf die Domäne verwendet werden: Wählen Sie auf der Registerkarte **Allgemein** im Dialogfeld **Eigenschaften** die entsprechende Option aus und klicken Sie dann auf **Anwenden**. Sie können eine der beiden Optionen wählen, die in Schritt 5 des Verfahrens oben aufgeführt sind.
- Das Container-Verzeichnis der **Verwalteten Domains** beinhaltet die angemeldeten Objekte aller bei Quest One ActiveRoles angemeldeten Domains. Sie können die Registrierung von Domänen aufheben, indem Sie Objekte aus diesem Container löschen.
- Im Auslieferungszustand sind bei Quest One ActiveRoles keine Domains angemeldet. Bei der Anmeldung einer Domain wird die Domain-Anmeldung als Teil der Einrichtungseinstellungen von Quest One ActiveRoles gespeichert.

Konfigurieren von nicht verwalteten Domänen

Bei der Anmeldung einer Active Directory-Domain bietet Quest One ActiveRoles die Möglichkeit, diese Domain als eine nicht verwaltete Domain zu verwenden. Diese Auswahlmöglichkeit ermöglicht Ihnen die Anmeldung einer Domain, ohne dass dabei die vollen Kosten für die Zulassung der in dieser Domain befindlichen Benutzerkonten zur Verwaltung durch Quest One ActiveRoles fällig werden.

Eine nicht verwaltete Domain ist im Grunde nichts anderes als eine bei Quest One ActiveRoles angemeldete schreibgeschützte Domain. Die Nutzung der Option einer nicht verwalteten Domäne ermöglicht Ihnen eine Reduzierung der Lizenzierungskosten, da die Benutzeranzahl, die den nicht verwalteten Domänen entspricht, nicht zur Gesamtanzahl der lizenzierten Benutzer hinzugefügt wird. Die einzige Bedingung ist, dass keine nicht verwaltete Domain mehr Benutzer beinhalten darf, als in der erworbenen Zulassung für Quest One ActiveRoles angegeben sind. Dies ermöglicht Ihnen, über eine beliebige Anzahl von nicht verwalteten Domänen zu verfügen, von denen jede so viele Benutzer wie in Ihrer Lizenz angegeben verfügt.

Wird die Auswahlmöglichkeit, eine Domain als nicht verwaltete Domain anzumelden, nicht gewählt, dann muss diese Domain auch dann, wenn Sie Quest One ActiveRoles lediglich zur Auflistung und Auswahl von Benutzerkonten aus einer bestimmten Domain benötigen, als gewöhnliche verwaltete Domain bei Quest One ActiveRoles angemeldet werden. Da für jedes freigeschaltete Benutzerkonto in den gewöhnlichen verwalteten Domains eine eigene Zulassung vorliegen muss, ist bei der Anmeldung einer weiteren Domain entsprechend eine Quest One ActiveRoles-Zulassung für eine Benutzerzahl, die großer ist als die Anzahl der freigeschalteten Benutzerkonten in den aktuell verwalteten Domains zuzüglich der Anzahl der freigeschalteten Benutzerkonten in der Domain, die hinzugefügt werden soll. Sie müssen mit anderen Worten weitere Benutzerzulassungen für Quest One ActiveRoles erwerben, auch wenn Sie nicht beabsichtigen, Quest One ActiveRoles zur Verwaltung der Benutzer in der Domain, die Sie anmelden mochten, zu verwenden.

Quest One ActiveRoles hat dieses Problem aufgegriffen und ermöglicht Ihnen die Anmeldung nicht verwalteter Domains. Durch die Verwendung der Möglichkeit, nicht verwaltete Domains anzumelden, hilft Quest One ActiveRoles in Fallen wie den nachfolgend aufgeführten die Kosten für Zulassungen zu senken:

- **Gruppenmitgliederverwaltung.** Bei der Verwendung zum Hinzufügen von Mitgliedern zu einer Gruppe durch Auswahl der neuen Mitglieder aus einer Aufstellung von Objekten benötigt Quest One ActiveRoles die die anzumeldenden Objekte enthaltende Domain. Wenn Quest One ActiveRoles lediglich zur Auswahl der Mitgliedsobjekte bei der Verwaltung der Gruppenmitglieder verwendet wird, kann die die Mitgliedsobjekte enthaltende Domain als nicht verwaltete Domain angemeldet werden.
- **Exchange-Ressourcenbestand.** Bei der Verwendung zur Bereitstellung von Exchange-Postfächern in einem anderen Bestand als dem, in dem sich die Konten der Postfachbenutzer befinden, setzt Quest One ActiveRoles voraus, dass die Domain der Postfachbesitzer (die Konten-Domain) angemeldet ist. Wenn Quest One ActiveRoles nicht zur Verwaltung der Benutzer in der Konten-Domain verwendet wird, kann diese als nicht verwaltete Domain angemeldet werden.

Bei der Anwendung auf eine angemeldete nicht verwaltete Domain sind die Funktionen und Eigenschaften von Quest One ActiveRoles auf solche beschrankt, die keinen Schreibzugriff auf die in der Domain befindlichen Objekte erfordern (einschließlich des Schreibzugriffs auf die von Quest One ActiveRoles als virtuelle Eigenschaften gespeicherten Objektdaten). Somit kann Quest One ActiveRoles verwendet werden, um:

- Suche nach, Auflisten und Auswählen von Objekten aus nicht verwalteten Domänen
- Füllen von Gruppen in normal verwalteten Domänen mit Objekten aus nicht verwalteten Domänen
- Abfragen und Anzeigen der Eigenschaften von Objekten, die sich in nicht verwalteten Domänen befinden
- Zuweisen von Benutzern oder Gruppen aus nicht verwalteten Domänen zur Rolle des Vorgesetzten, primären Besitzers oder sekundären Besitzers für Objekte, die sich in normal verwalteten Domänen befinden
- Verwaltungsaufgaben und Freigabevorgange an Benutzer oder Gruppen in nicht verwalteten Domains zu delegieren
- die Richtlinien von Quest One ActiveRoles auf Objekte in nicht verwalteten Domains anzuwenden, wenn diese Richtlinien keinen Schreibzugriff auf diese Objekte benötigen
- Bereitstellen von Benutzern aus nicht verwalteten Domänen mit verknüpften Exchange-Postfächern, die sich in einer separaten verwalteten Gesamtstruktur befinden
- Füllen von verwalteten Einheiten mit Objekten aus nicht verwalteten Domänen

Aufgrund des schreibgeschützten Zugriffs auf nicht verwaltete Domains kann Quest One ActiveRoles nicht verwendet werden, um:

- Erstellen, Verschieben oder Löschen von Objekten in nicht verwalteten Domänen
- Ändern jeglicher Eigenschaften von Objekten, die sich in nicht verwalteten Domänen befinden
- Ausführen jeglicher mit der Gruppenmitgliedschaft in Verbindung stehender Richtlinien für die Gruppen in nicht verwalteten Domänen einschließlich der für Gruppenfamilien und dynamische Gruppen geltenden Richtlinien
- Ausführen jeglicher automatischer Bereitstellungsrichtlinien oder Deprovisionierungsrichtlinien für Benutzer oder Gruppen, die sich in nicht verwalteten Domänen befinden
- Ausführen jeglicher Arbeitsabläufe, die Änderungen an Objekten in nicht verwalteten Domänen vornehmen
- Wiederherstellen von Objekten aus dem Active Directory-Papierkorb in nicht verwalteten Domänen

Lizenzieren von nicht verwalteten Domänen

Eine nicht verwaltete Domain ist im Grunde nichts anderes als eine bei Quest One ActiveRoles angemeldete schreibgeschützte Domain. Wenn Quest One ActiveRoles nicht zur Vornahme von Änderungen an einer Domain verwendet wird, sondern in dieser Domain lediglich Objekte auswählen und Daten abrufen muss, kann diese als nicht verwaltete Domain angemeldet werden, um die Kosten für Zulassungen zu senken. Die Senkung der Zulassungskosten verdankt sich dem Umstand, dass Quest One ActiveRoles die Benutzer in den nicht verwalteten Domains getrennt von den Benutzern in den übrigen Domains erfasst, was zwei Benutzerzahlen nach sich zieht: eine Zahl für die normal verwalteten Domänen (die ohne die Verwendung der Option der nicht verwalteten Domäne registrierten) und eine weitere für die nicht verwalteten Domänen. Das von Quest One ActiveRoles gepflegte Zulassungsmodell verlangt, dass die Gesamtzahl der freigeschalteten Benutzerkonten in den gewöhnlichen verwalteten Domains die zugelassene Benutzerzahl nicht übersteigt, diese Vorgabe gilt jedoch nicht für die nicht verwalteten Domains. Die Anzahl der Benutzer in jeder nicht verwalteten Domäne wird separat und unabhängig von der Benutzerzahl in den normal verwalteten Domänen ermittelt. Ungeachtet der Anzahl der Benutzer in den gewöhnlichen verwalteten Domains kann in Quest One ActiveRoles jede nicht verwaltete Domain eine beliebige Zahl freigeschalteter Benutzerkonten enthalten, solange die zugelassene Benutzerzahl nicht überschritten wird.

Quest One ActiveRoles ermöglicht das Anlegen einer beliebigen Anzahl nicht verwalteter Domains, solange die Zahl der freigeschalteten Benutzerkonten in den einzelnen nicht verwalteten Domains die in Ihrer Zulassung für Quest One ActiveRoles ausgewiesene Benutzerzahl nicht überschreitet. Wenn Ihre Lizenz zum Beispiel 10.000 Benutzer zulässt, dann können Sie jede beliebige Anzahl von nicht verwalteten Domänen hinzufügen, wobei jede dieser Domänen höchstens 10.000 aktivierte Benutzerkonten umfassen darf. Ohne die Möglichkeit, nicht verwaltete Domains anzumelden, dürfen alle bei Quest One ActiveRoles angemeldeten Domains insgesamt höchstens 10.000 freigeschaltete Benutzerkonten umfassen.

Kurz gesagt, für die Lizenzierung der nicht verwaltete Domänen wird zunächst die Anzahl der aktivierten Benutzerkonten in jeder nicht verwalteten Domäne ermittelt und anschließend die Domäne mit der größten Anzahl herangezogen. Diese Anzahl darf die in der Lizenz angegebene Anzahl nicht überschreiten. Angenommen, bei Quest One ActiveRoles wurden zwei nicht verwaltete Domains angemeldet, von denen die eine 5.000 freigeschaltete Benutzerkonten enthalt und die andere 10.000. In diesem Fall wird die höhere Zahl berücksichtigt, es ist also eine Quest One ActiveRoles-Zulassung für mindestens 10.000 Benutzer erforderlich.

Übersteigt die Anzahl der freigeschalteten Benutzerkonten in einer der angemeldeten nicht verwalteten Domains die in der Zulassung ausgewiesene Zahl, so erscheint beim Öffnen der Programmsteuerung oder der Web-Schnittstelle von Quest One ActiveRoles durch den Benutzer automatisch eine Warnmeldung, die auf den Verstoß gegen die Zulassung hinweist. In diesem Fall muss der Benutzer einen Quest-Vertreter kontaktieren, um die entsprechende Anzahl von Benutzerlizenzen zu erwerben, die zur Gewährleistung der Konformität mit den Lizenzbedingungen erforderlich ist.

Registrieren einer nicht verwalteten Domäne

Nicht verwaltete Domains können mithilfe der Quest One ActiveRoles-Programmsteuerung angemeldet werden. Der Assistent zum Hinzufügen einer verwalteten Domäne bietet die entsprechende Option auf der Seite, auf der Sie die zu registrierende Domäne auswählen.

Gehen Sie folgendermaßen vor, um eine nicht verwaltete Domäne zu registrieren:

1. Wahlen Sie im Baum der Programmsteuerung den **Quest One ActiveRoles**-Stammknoten.
2. Klicken Sie dann im Angabenfenster auf die Schaltflache **Domain hinzufügen**, um den Assistenten zur Anmeldung einer Domain aufzurufen.
3. Geben Sie auf der Seite **Domänenauswahl** im Assistenten den DNS-Namen der zu registrierenden Domäne ein und aktivieren Sie dann das Kontrollkästchen **Als nicht verwaltete Domäne verwenden**.
4. Folgen Sie den Anweisungen des Assistenten, um die Registrierung der Domäne abzuschließen.

Warten Sie nach Fertigstellung des Assistenten, bis Quest One ActiveRoles die Angaben zu der neu hinzugefügten Domain zusammengetragen hat. Verwenden Sie den Befehl **Aktualisieren**, um den angezeigten Domänenstatus zu aktualisieren. Nach Abschluss des Zusammentragens der Domain-Angaben erscheint neben dem Namen der Domain der Hinweis **Als nicht verwaltete Domain verfügbar** im Bereich der **Domains** auf der Stammseite von Quest One ActiveRoles.

- Wenn die Option **Als nicht verwaltete Domäne verwenden** im Assistenten ausgewählt ist, kann sie nach der Registrierung der Domäne nicht mehr geändert werden. Wenn Sie nicht mehr möchten, dass eine Domäne nicht verwaltet wird, müssen Sie die Registrierung der Domäne aufheben (das entsprechende Objekt im Container **Verwaltete Domänen** löschen) und die Domäne dann erneut registrieren, wobei Sie die Option **Als nicht verwaltete Domäne verwenden** deaktiviert lassen.
- Alle bei Quest One ActiveRoles angemeldeten Domains werden im **Domains**-Bereich der Quest One ActiveRoles-Stammseite in der Programmsteuerung aufgeführt. Um nicht verwaltete Domänen zu erkennen, wird der Hinweistext **Als nicht verwaltete Domäne verfügbar** neben dem Namen jeder nicht verwalteten **Domäne** im Bereich Domänen angezeigt. Neben den Namen der normal verwalteten Domänen steht der Hinweistext **Verfügbar für die Verwaltung**.
- Der Hinweis auf eine nicht verwaltete Domäne erfolgt auch auf der Registerkarte **Allgemein** im Dialogfeld **Eigenschaften** für jedes im Container **Verwaltete Domänen** enthaltene Domänenregistrierungsobjekt. In diesem Fall handelt es sich um ein nicht aktivierbares bzw. deaktivierbares Kontrollkästchen mit der Bezeichnung **Als nicht verwaltete Domäne verwenden**. Das Kontrollkästchen ist automatisch aktiviert, wenn die Domäne nicht verwaltet ist. Falls die Domäne verwaltet ist, ist das Kontrollkästchen deaktiviert. Da der Status einer Domäne (nicht verwaltet oder normal verwaltet) nur bei der Registrierung der Domäne gesetzt werden kann, kann das Kontrollkästchen **Als nicht verwaltete Domäne verwenden** nicht auf der Registerkarte **Allgemein** aktiviert bzw. deaktiviert werden.

Konfigurieren der Replikation

Quest One ActiveRoles nutzt die Replikationsfunktion von Microsoft SQL Server zum Kopieren und zur Weitergabe von Einrichtungseinstellungsdaten aus einer Verwaltungsdienstdatenbank an eine andere sowie zum Synchronisieren der Datenbanken zur Konsistenzsicherung.

Datenbankserver des Verwaltungsdienstes, die mit Hilfe der Replikationsfunktionalität von SQLServer synchronisiert werden, werden als *Replikationspartner* bezeichnet. Jeder Replikationspartner pflegt eine schreibbare Kopie der Konfigurationsdaten des Dienstes. Wenn Änderungen an einem Replikationspartner vorgenommen werden, werden diese auch an die anderen Replikationspartner weitergegeben.

Grundlegendes zum Replikationsmodell

In einer Quest One ActiveRoles-Umgebung wird die Replikationsfunktion von SQL Server verwendet, um Änderungen an den Daten der Einrichtungseinstellungen an alle Mitglieder des Replikationsverteilers weiterzugeben, sobald die Daten auf einem der Mitgliedsrechner dieses Verteilers geändert werden. Der Replikationsvorgang wird unmittelbar nach der Vornahme der Änderungen durch ein Mitglied des Replikationsverteilers ausgelost. Quest One ActiveRoles bietet keine Möglichkeit, dieses Verhalten zu ändern.

Da normalerweise nur wenige Änderungen vorliegen und da bei der Replikation nur geänderte Daten weitergegeben werden (Mergerreplikation), ist der Datenverkehr für die Replikation überschaubar. Deshalb muss das Replizieren in Quest One ActiveRoles weder geplant noch von Hand erzwungen werden.

Bei der Mergereplikation ist normalerweise ein Lösungsmechanismus für Konflikte notwendig, die entstehen, wenn die gleichen Daten auf unterschiedlichen Replikationspartnern unterschiedlich geändert werden. In dem Replikationsmodell von Quest One ActiveRoles werden Konflikte nach dem Prinzip „Wer zuletzt kommt, gewinnt" entschieden, das bedeutet, die zeitlich zuletzt vorgenommene Änderung an den Daten wird angewendet.

In dem Replikationsmodell von Quest One ActiveRoles kann jede Datenbank des Verwaltungsdienstes eine der folgenden Funktionen erfüllen:

- **Herausgeber.** Der Publisher (Herausgeber) ist der Datenbankserver, der Daten für die Replikation anderen Replikationspartner verfügbar macht.

  Der Verwaltungsdienst, der den Publisher-Datenbankserver verwendet, wird als *Publisher-Verwaltungsdienst* bezeichnet.

- **Abonnent.** Abonnenten sind Datenbankserver, die replizierte Daten empfangen. Abonnenten können Datenänderungen vom Publisher empfangen sowie Datenänderungen zurück an den Publisher weitergeben.

  Der Verwaltungsdienst, der einen Abonnenten-Datenbankserver verwendet, wird als *Abonnenten-Verwaltungsdienst* bezeichnet.

Replikationsgruppe

Der Publisher und seine Abonnenten bilden zusammen eine Replikationsgruppe. Jede Replikationsgruppe muss genau einen Publisher enthalten und kann beliebig viele Abonnenten enthalten. Die Mitglieder einer Replikationsgruppe werden als *Replikationspartner* bezeichnet.

Jedes Mitglied einer Replikationsgruppe (jeder Replikationspartner) pflegt eine eigene, schreibbare Kopie der Konfigurationsdaten des Verwaltungsdienstes. Die Replikation kopiert und verteilt Daten zwischen Mitgliedsdatenbanken und synchronisiert im Interesse der Konsistenz Daten zwischen den Datenbanken. Wenn Änderungen auf dem Publisher vorgenommen werden, repliziert der Publisher sie an jeden Abonnenten. Wenn Datenänderungen auf einem Abonnenten vorgenommen werden, leitet der Abonnent sie an den Publisher weiter, der sie dann an jeden Abonnenten repliziert.

Dieser Replikationsprozess stellt sicher, dass alle Verwaltungsdienste, die die Datenbankserver in der Replikationsgruppe verwenden, die gleiche Konfiguration aufweisen.

Wenn ein Datenbankserver mit dem Verwaltungsdienst eingerichtet wird, wird er zunächst als *allein stehende Datenbank* konfiguriert. Er hat also keine Replikationspartner und gehört keiner Replikationsgruppe an. Der Verwaltungsdienst, der einen allein stehenden Datenbankserver verwendet, wird als *allein stehender Verwaltungsdienst* bezeichnet.

Sie können einen allein stehenden Datenbankserver einer beliebigen vorhandenen Replikationsgruppe hinzufügen. Dann wird der Datenbankserver ein Abonnent. Jeder Datenbankserver mit dem Verwaltungsdienst darf nur einer Replikationsgruppe angehören. Nachdem er aus einer Replikationsgruppe entfernt wurde, kann er einer anderen hinzugefügt werden.

Um eine neue Replikationsgruppe zu erstellen, muss ein allein stehender Datenbankserver als Publisher ausgewählt werden. Dann enthält die neue Replikationsgruppe ein einziges Mitglied, den Publisher. Später können Sie der Gruppe Abonnenten hinzufügen.

Beim Auftreten von Fehlern beim Replizieren in Quest One ActiveRoles weist die Quest One ActiveRoles -Programmsteuerung optisch auf dieses Problem hin, indem sie die Symbole der Container für die **Servereinstellungen** und die**Einstellungsdatenbanken** im Baum der Programmsteuerung ändert: Neben jedem dieser Container wird eine Beschriftung mit einem Ausrufezeichen angezeigt. So kann der Administrator einen Replikationsfehler erkennen, ohne einzelne Replikationspartner zu untersuchen.

Konfigurieren von SQL Server

Um sicherzustellen, dass SQL Server für die Verwaltungsdienstreplikation ordnungsgemäß konfiguriert ist, prüfen Sie, ob der SQL Server-Agent-Dienst gestartet wurde und ordnungsgemäß konfiguriert ist.

Der SQL Server-Agentendienst muss auf dem Datenbankserver mit SQL Server ausgeführt werden, der als Publisher dient. Sie sollten den Starttyp für diesen Dienst auf **Automatisch** festlegen.

Der SQL Server-Agentendienst sollte so konfiguriert sein, dass er sich mit einem Domänenbenutzerkonto anmeldet. Das Anmeldekonto für den Dienst muss über ausreichende Rechte verfügen, um eine Verbindung zu dem SQL-Server des Herausgebers (Publisher) und dem SQL-Server des Abonnenten (Subscriber) herzustellen (s. „Berechtigungen des Replikationsagenten“ in der Kurzanleitung zur Inbetriebnahme von *Quest One ActiveRoles „Erste Schritte*“).

Erstellen einer Replikationsgruppe

Um eine Replikationsgruppe zu erstellen, wählen Sie einen allein stehenden Datenbankserver mit dem Verwaltungsdienst als Publisher aus. Das kann mithilfe der Programmsteuerung von Quest One ActiveRoles erfolgen:

1. Stellen Sie eine Verbindung zu einem autonomen Verwaltungsdienst her.
2. Stufen Sie den Datenbankserver mit dem Verwaltungsdienst zum Publisher herauf.

Um eine Verbindung zum Verwaltungsdienst herzustellen, gehen Sie gemäß den weiter oben in diesem Kapitel aufgeführten Anweisungen vor (siehe Herstellen einer Verbindung zum Verwaltungsdienst).

Nachdem Sie eine Verbindung mit dem Verwaltungsdienst hergestellt haben, führen Sie die folgenden Schritte aus, um die Verwaltungsserver-Datenbank zum Publisher heraufzustufen:

1. Wechseln Sie in der Konsolenstruktur zum Container **Configuration/Server Configuration/Configuration Databases**.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf die Datenbank und klicken Sie dann auf **Heraufstufen**.

Der Befehl **Heraufstufen** wird nur angezeigt, wenn der Verwaltungsdienst einen allein stehenden Datenbankserver verwendet, d.h. einen Datenbankserver, der keiner Replikationsgruppe angehört.

Nachdem Sie auf **Heraufstufen** geklickt haben, dauert das Abschließen des Vorgangs mehrere Minuten. Nach Abschluss des Vorgangs enthält die neue Replikationsgruppe ein einziges Mitglied, den Publisher. Nach der Erstellung der Replikationsgruppe können Sie ihren Replikationspartner hinzufügen, die Abonnenten.

Sollte Quest One ActiveRoles nicht über ausreichende Rechte verfügen, um den Vorgang zum **Heraufstufen** auf dem SQL-Server auszufuhren, dann fordert die Quest One ActiveRoles-Programmsteuerung Sie auf, für diesen Vorgang ein anderes Konto bereitzustellen (s. „Berechtigungen zum Anlegen oder Loschen des Herausgebers (Publisher)" in der Kurzanleitung zur Inbetriebnahme von *Quest One ActiveRoles „Erste Schritte*").

Hinzufügen von Mitgliedern zu einer Replikationsgruppe

Um einer Replikationsgruppe ein Mitglied hinzuzufügen, wählen Sie einen allein stehenden Datenbankserver als Abonnenten des Publishers der Gruppe aus. Das kann mithilfe der Programmsteuerung von Quest One ActiveRoles erfolgen:

1. Stellen Sie eine Verbindung zum Publisher-Verwaltungsdienst her.
2. Starten Sie den Assistenten „Neuer Replikationspartner" und schließen Sie ihn ab.

Zeigen Sie nach dem Herstellen der Verbindung zum Publisher-Verwaltungsdienst den Inhalt des Containers **Configuration Databases** an. Im Bereich „Details" werden die Namen des Publisher und seiner Abonnenten aufgelistet. Klicken Sie mit der rechten Maustaste auf den Publisher und klicken Sie dann auf **Replikationspartner hinzufügen**. Folgen Sie dann den Anweisungen des Assistenten „Neuer Replikationspartner".

Klicken Sie auf der Seite **Datenbankauswahl** auf **Durchsuchen**, um den Verwaltungsdienst auszuwählen, der den als Abonnenten vorgesehenen Datenbankserver verwendet. Durch Anklicken von **Durchsuchen** wird ein Dialogfeld angezeigt, das mit dem im Abschnitt Herstellen einer Verbindung zum Verwaltungsdienst weiter oben in diesem Kapitel beschriebenen Dialogfeld identisch ist. Geben Sie den Namen des Computers mit dem Verwaltungsdienst ein, oder wählen Sie ihn in der Liste aus.

Der Assistent wählt automatisch den Datenbankserver aus, auf dem die Datenbank des von Ihnen angegebenen Verwaltungsdienstes untergebracht wird. Wenn Quest One ActiveRoles nicht über ausreichende Rechte zur Ausführung des Vorgangs **Zum Replikationsverteiler hinzufügen** auf dem SQL-Server verfügt, fordert der Assistent Sie auf, für diesen Vorgang ein anderes Konto bereitzustellen (s. „Berechtigungen zum Anlegen oder Loschen eines Abonnenten (Subscriber)" in der Kurzanleitung zur Inbetriebnahme von *Quest One ActiveRoles „Erste Schritte*").

Die nächste Seite des Assistenten zeigt den aus dem angegebenen Verwaltungsdienst abgerufenen Namen und den Netzwerkstandort der Datenbank an und fordert Sie zur Auswahl einer der folgenden Möglichkeiten zur Herstellung der Verbindung zwischen dem Replikationsagenten auf dem SQL-Server des Herausgebers (Publisher) und dem SQL-Server des Abonnenten (Subscriber) Auszuwahlen:

- **Das Konto des SQL-Server-Agentendienstes imitieren.** Diese Möglichkeit sollte eingeschaltet werden, wenn der SQL-Server-Agentendienst auf dem SQL-Server des Herausgebers so eingerichtet wurde, dass es sich als mit ausreichenden Rechten auf dem SQL-Server des Abonnenten versehenes Windows-Benutzerkonto anmeldet. Durch Auswahl dieser Möglichkeit stellt der Replikationsagent unter dem Anmeldekonto des auf dem SQL-Server des Herausgebers laufenden SQL-Server-Agentendienstes eine Verbindung zu dem SQL-Server des Abonnenten her.
- **Die Bestätigung der Zugriffsberechtigung auf den SQL-Server mit folgendem Benutzernamen und Passwort verwenden.** Diese Möglichkeit sollte genutzt werden, wenn das Anmeldekonto des SQL-Server-Agentendienstes nicht mit den erforderlichen Rechten auf dem SQL-Server des Herausgebers eingerichtet werden kann. Sie werden zur Angabe des SQL-Server-Benutzernamens und -Passworts aufgefordert, die der auf dem SQL-Server des Herausgebers laufende Replikationsagenten zur Herstellung einer Verbindung mit dem SQL-Server des Abonnenten verwenden soll.

Das von dem Replikationsagenten zur Herstellung einer Verbindung mit dem SQL-Server des Herausgebers verwendete Konto muss mindestens Mitglied der festen **db_owner**-Datenbankberechtigungsgruppe in der Abonnementsdatenbank (Quest One ActiveRoles-Abonnentendatenbank) sein. Weitere Hinweise dazu finden Sie unter „Berechtigungen des Replikationsagenten" in der Kurzanleitung zur Inbetriebnahme von *Quest One ActiveRoles „Erste Schritte*".

Auf der Abschlussseite des Assistenten können Sie Zusammenfassungsinformationen zu dem Datenbankserver überprüfen, den Sie als Abonnenten einrichten möchten. Nachdem Sie auf **Fertig stellen** klicken, wird der Datenbankserver der Replikationsgruppe hinzugefügt. Der Replikationsprozess aktualisiert die Datenbank des neuen Abonnenten mit den Daten, die vom Publisher abgerufen wurden.

Der Publisher kopiert neue Daten in die Datenbank und überschreibt dabei die vorhandenen Daten. Wenn die Datenbank wichtige Informationen (z.B. benutzerdefinierte Zugriffsvorlagen oder Richtlinienobjekte) enthält, sollten Sie diese Objekte exportieren, bevor Sie den Datenbankserver als Abonnenten festlegen, und sie nach Abschluss des Vorgangs wieder importieren.

Verfahren zum Hinzufügen von Mitgliedern zu einer Replikationsgruppe

Um einer Replikationsgruppe ein Mitglied hinzuzufügen, wählen Sie einen allein stehenden Datenbankserver als Abonnenten des Publishers der Gruppe aus.

So fügen Sie einen Replikationspartner zu einer Replikationsgruppe hinzu:

1. Stellen Sie eine Verbindung zu dem Verwaltungsdienst her, dessen Datenbankserver die Herausgeber-Rolle inne hat.

   Anweisungen bezüglich des Aufbaus einer Verbindung zum Verwaltungsdienst finden Sie unter Herstellen einer Verbindung zum Verwaltungsdienst weiter oben in diesem Kapitel.

2. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Server Configuration** und klicken Sie dann auf **Configuration Databases.**
3. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf den Herausgeber und klicken Sie dann auf **Replikationspartner hinzufügen**.
4. Folgen Sie den Anweisungen des Assistenten zum Erstellen eines neuen Replikationspartners.
5. Klicken Sie auf der Seite **Datenbankauswahl** auf **Durchsuchen**.
6. Verwenden Sie das Dialogfeld **Verbindung zum Verwaltungsdienst herstellen**, um den Verwaltungsdienst auszuwählen, dessen SQL Server als ein Abonnent dieses Herausgebers konfiguriert werden soll.

   *Wenn Quest One ActiveRoles nicht über ausreichende Rechte zur Ausführung des Vorgangs **Zum Replikationsverteiler hinzufügen** auf dem SQL-Server verfügt, fordert der Assistent Sie auf, für diesen Vorgang ein anderes Konto bereitzustellen (s. „Berechtigungen zum Anlegen oder Loschen eines Abonnenten (Subscriber)" in der Kurzanleitung zur Inbetriebnahme von Quest One ActiveRoles „Erste Schritte").*

   Die nächste Seite des Assistenten zeigt den aus dem angegebenen Verwaltungsdienst abgerufenen Namen und den Netzwerkstandort der Datenbank an und fordert Sie zur Auswahl einer der folgenden Möglichkeiten zur Herstellung der Verbindung zwischen dem Replikationsagenten auf dem SQL-Server des Herausgebers (Publisher) und dem SQL-Server des Abonnenten (Subscriber) Auszuwahlen

7. Wählen Sie eine dieser Optionen aus:
   - **Das Konto des SQL-Server-Agentendienstes imitieren.** Diese Möglichkeit sollte gewählt werden, wenn der SQL-Server-Agentendienst auf dem SQL-Server des Herausgebers so eingerichtet wurde, dass es sich als mit ausreichenden Rechten auf dem SQL-Server des Abonnenten versehenes Windows-Benutzerkonto anmeldet. Durch Auswahl dieser Möglichkeit stellt der Replikationsagent unter dem Anmeldekonto des auf dem SQL-Server des Herausgebers laufenden SQL-Server-Agentendienstes eine Verbindung zu dem SQL-Server des Abonnenten her.
   - **Die Bestätigung der Zugriffsberechtigung auf den SQL-Server mit folgendem Benutzernamen und Passwort verwenden.** Diese Möglichkeit sollte gewählt werden, wenn das Anmeldekonto des SQL-Server-Agentendienstes nicht mit den erforderlichen Rechten auf dem SQL-Server des Herausgebers eingerichtet werden kann. Sie werden zur Angabe des SQL-Server-Benutzernamens und -Passworts aufgefordert, die der auf dem SQL-Server des Herausgebers laufende Replikationsagenten zur Herstellung einer Verbindung mit dem SQL-Server des Abonnenten verwenden soll.

   *Das von dem Replikationsagenten zur Herstellung einer Verbindung mit dem SQL-Server des Herausgebers verwendete Konto muss mindestens Mitglied der festen **db_owner**-Datenbankberechtigungsgruppe in der Abonnementsdatenbank (Quest One ActiveRoles-Abonnentendatenbank) sein. Weitere Hinweise dazu finden Sie unter „Berechtigungen des Replikationsagenten" in der Kurzanleitung zur Inbetriebnahme von Quest One ActiveRoles „Erste Schritte".*

8. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

- Nachdem Sie auf **Fertig stellen** klicken, wird der Datenbankserver der Replikationsgruppe hinzugefügt. Der Replikationsprozess aktualisiert die Datenbank des neuen Abonnenten mit den Daten, die vom Publisher abgerufen wurden.
- Der Publisher kopiert neue Daten in die Datenbank und überschreibt dabei die vorhandenen Daten. Wenn die Datenbank wertvolle Informationen enthält (z. B. eine benutzerdefinierte Zugriffsvorlage oder Richtlinienobjekte), sollten Sie diese exportieren, bevor Sie die Datenbank als Abonnent festlegen, und später, nach Abschluss des Vorgangs, wieder zurückimportieren.
- Eine Datenbank kann nicht als Replikationsgruppe hinzugefügt werden, wenn Sie bereits einer anderen Replikationsgruppe angehört. Wenn Sie die Datenbank zu einer anderen Replikationsgruppe hinzufügen möchten, müssen Sie sie zuerst aus der aktuellen Replikationsgruppe entfernen.

Entfernen von Mitgliedern aus einer Replikationsgruppe

Mithilfe der Programmsteuerung von Quest One ActiveRoles können Abonnenten aus einer Replikationsgruppe entfernt werden:

1. Stellen Sie eine Verbindung zum Publisher-Verwaltungsdienst her.
2. Wählen Sie im Container **Configuration Databases** einen Abonnenten aus, klicken Sie mit der rechten Maustaste auf den Abonnenten und klicken Sie dann auf **Löschen**.

Sollte Quest One ActiveRoles nicht über ausreichende Rechte zur Ausführung des Vorgangs auf dem SQL-Server verfügen, dann werden Sie von der Quest One ActiveRoles-Programmsteuerung aufgefordert, für diesen Vorgang ein anderes Konto bereitzustellen (s. „Berechtigungen zum Anlegen oder Loschen eines Abonnenten (Subscriber)“ in der Kurzanleitung zur Inbetriebnahme von *Quest One ActiveRoles „Erste Schritte*“).

Mit dieser Methode können Sie nur Abonnenten entfernen. Der Publisher kann nicht aus seiner Replikationsgruppe entfernt werden, während sie Abonnenten enthält.

Um den Publisher zu entfernen, müssen Sie erst alle Abonnenten entfernen und dann den Publisher herabstufen. Diese Aktion löscht die gesamte Replikationsgruppe.

Nachdem Sie alle Abonnenten entfernt haben, können Sie den Publisher wie folgt herabstufen: Klicken Sie im Container **Configuration Databases** mit der rechten Maustaste auf den Publisher und klicken Sie dann auf **Herabstufen**.

Sollte Quest One ActiveRoles nicht über ausreichende Rechte verfügen, um den Vorgang zum **Zurückstufen** auf dem SQL-Server auszufuhren, dann fordert die Quest One ActiveRoles-Programmsteuerung Sie auf, für diesen Vorgang ein anderes Konto bereitzustellen (s. „Berechtigungen zum Anlegen oder Loschen des Herausgebers (Publisher)“ in der Kurzanleitung zur Inbetriebnahme von *Quest One ActiveRoles „Erste Schritte*“).

Verfahren zum Entfernen von Mitgliedern aus einer Replikationsgruppe

So entfernen Sie Abonnenten aus einer Replikationsgruppe:

1. Stellen Sie eine Verbindung zum Publisher-Verwaltungsdienst her.
2. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Server Configuration** und klicken Sie dann auf **Configuration Databases.**
3. Klicken Sie im Bereich „Details“ mit der rechten Maustaste auf das Computerkonto und klicken Sie dann auf **Löschen**.

So entfernen Sie den Publisher aus einer Replikationsgruppe:

1. Stellen Sie eine Verbindung zum Publisher-Verwaltungsdienst her.
2. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Server Configuration** und klicken Sie dann auf **Configuration Databases.**
3. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf den Publisher und klicken Sie dann auf **Herabstufen**.

- Weitere Informationen über den Aufbau einer Verbindung zum Verwaltungsdienst finden Sie unter Herstellen einer Verbindung zum Verwaltungsdienst weiter oben in diesem Kapitel.
- Der Publisher kann nicht aus seiner Replikationsgruppe entfernt werden, während sie Abonnenten enthält. Um den Publisher zu entfernen, müssen Sie erst alle Abonnenten entfernen und dann den Publisher herabstufen. Dieser Vorgang löscht die Replikationsgruppe. Nachdem Sie alle Abonnenten entfernt haben, können Sie den Publisher wie folgt herabstufen:
- Der Befehl **Herabstufen** wird nur angezeigt, wenn der Herausgeber das einzige Mitglied der Replikationsgruppe ist.
- Wenn Quest One ActiveRoles nicht über ausreichende Rechte zur Ausführung des Vorgangs auf dem SQL-Server verfügt, fordert die Programmsteuerung von Quest One ActiveRoles Sie auf, für diesen Vorgang ein anderes Konto bereitzustellen (s. „Berechtigungen zur Einrichtung der Replikation" in der Kurzanleitung zur Inbetriebnahme von *Quest One ActiveRoles „Erste Schritte*").

Überwachung der Replikation

Quest One ActiveRoles ermöglicht die Überwachung des jeweiligen Status' der Mitglieder des Replikationsverteilers. Mithilfe der Überwachung kann ermittelt werden, ob die Replikation in Quest One ActiveRoles erfolgreich und fehlerfrei funktioniert. Der Status eines Replikationspartners kann über die Programmsteuerung von Quest One ActiveRoles angezeigt werden:

1. Stellen Sie eine Verbindung mit einem beliebigen Verwaltungsdienst in der Replikationsgruppe her.
2. Öffnen Sie das Dialogfeld **Eigenschaften** für den Replikationspartner und öffnen Sie die Registerkarte **Replikationsstatus**.

Um eine Verbindung zum Verwaltungsdienst herzustellen, gehen Sie gemäß den weiter oben in diesem Kapitel aufgeführten Anweisungen vor (siehe Herstellen einer Verbindung zum Verwaltungsdienst).

Nachdem Sie eine Verbindung mit dem Verwaltungsdienst hergestellt haben, öffnen Sie in den folgenden Schritten das Dialogfeld **Eigenschaften** für einen Replikationspartner:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Server Configuration** und wählen Sie dann **Configuration Databases**.
2. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf den Replikationspartner und klicken Sie dann auf **Eigenschaften**.

Im Dialogfeld **Eigenschaften** werden auf der Registerkarte **Replikationsstatus** Information zur letzten Replikationsaktion des Partners bereitgestellt, und es wird angezeigt, ob die Aktion erfolgreich abgeschlossen wurde, einen Fehler generiert hat oder noch ausgeführt wird.

Beim Auftreten von Fehlern beim Replizieren in Quest One ActiveRoles weist die Quest One ActiveRoles -Programmsteuerung optisch auf dieses Problem hin, indem sie die Symbole der Container für die **Servereinstellungen** und die**Einstellungsdatenbanken** im Baum der Programmsteuerung verändert. So können Sie einen Replikationsfehler erkennen, ohne einzelne Datenbanken zu untersuchen.

Weitere Hinweise zur Überwachung der Funktionsfähigkeit der Replikation in Quest One ActiveRoles finden Sie unter *Quest One ActiveRoles-Replikation: Empfohlene Vorgehensweisen und Fehlerbehebung*.

Verwenden der Datenbankspiegelung

Ab der Ausgabe 6.5 ist Quest One ActiveRoles in der Lage, die Datenbankspiegelungstechnologie von Microsoft SQL Server zur Verbesserung der Verfugbarkeit des Verwaltungsdienstes einzusetzen. Die Datenbankspiegelung bietet einen Standby-Datenbankserver, der Failover unterstützt. Wenn der aktuelle Datenbankserver ausfällt, kann der Verwaltungsdienst schnell durch einen automatischen Verbindungsaufbau zum Standby-Server wiederhergestellt werden (dieser Vorgang wird als „Failover" bezeichnet).

Die Datenbankspiegelung erhöht die Datenbankverfügbarkeit durch Unterstützung eines schnellen Failovers. Diese Technologie kann zur Pflege von zwei Kopien einer einzigen Quest One ActiveRoles-Datenbank auf unterschiedlichen Serverinstanzen des SQL-Server-Datenbankmoduls verwendet werden. Eine Serverinstanz bedient die Datenbank für den Verwaltungsdienst; diese Instanz wird als *Hauptserver* bezeichnet. Die andere Instanz fungiert als ein Standby-Server; diese Instanz wird als *Spiegelserver* bezeichnet.

Funktionswechsel

Im Zusammenhang mit der Datenbankspiegelung fungiert der Spiegelserver als der Failover-Partner für den Hauptserver. Bei einem Notfall übernimmt der Spiegelserver die Funktion des Hauptservers und stellt die gespiegelte Kopie der Datenbank als neue Hauptdatenbank online. Der ehemalige Hauptserver übernimmt dann, sofern er wieder verfügbar ist, die Funktion des Spiegelservers. Dieser als *Funktionswechsel* bekannte Vorgang kann in folgender Form erfolgen:

- **Automatischer Failover.** Wenn der Hauptserver ausfällt, wird bei Auswahl dieser Option die gespiegelte Kopie der Datenbank schnell als neue Hauptdatenbank online verfügbar gemacht.
- **Manueller Failover.** Ermöglicht dem Datenbankbesitzer, die Funktionen der Failover-Partner bei Bedarf umzukehren.
- **Forcierter Dienst.** Wenn der Hauptserver ausfällt, ermöglicht diese Option dem Datenbankbesitzer, den Zugriff auf die Datenbank wiederherzustellen, indem er den Spiegelserver zur Übernahme der Funktion des Hauptservers zwingt.

Bei jedem Funktionswechsel kann der Verwaltungsdienst, sobald der neue Hauptdatenbank online ist, wiederhergestellt werden, indem er automatisch wieder die Verbindung zur Datenbank aufbaut.

Weitere Hinweise zur Datenbankspiegelungstechnologie sowie Anleitungen zur Einrichtung und Anwendung der Datenbankspiegelung auf dem SQL-Server finden Sie in den Punkten zur „Datenbankspiegelung" in den Produktunterlagen zu dem SQL-Server unter http://msdn.microsoft.com/en-us/library/bb934127.aspx.

In der Version 6.x wird die Replikationsfunktion von Quest One ActiveRoles bei Datenbanken mit eingerichteter Spiegelung nicht unterstutzt. Wenn Sie versuchen, den Vorgang „An Herausgeber veröffentlichen" oder „Abonnent hinzufügen" für eine solche Datenbank durchzuführen, wird ein Fehler ausgegeben.

Einrichtung der Datenbankspiegelung in Quest One ActiveRoles

Wir setzen hier voraus, dass die Spiegelung für die Quest One ActiveRoles-Datenbank aufseiten des SQL-Servers in Übereinstimmung mit den Empfehlungen und Anleitungen der Unterlagen von Microsoft bereits eingerichtet worden ist, sodass die folgenden Bedingungen erfüllt sind:

- Der Verwaltungsdienst ist mit der Konfigurationsdatenbank auf dem Hauptdatenbankserver verbunden.
- Für die Einrichtungseinstellungendatenbank wurde keine Replikation eingerichtet (der Datenbankserver fungiert in Bezug auf die Quest One ActiveRoles-Replikation als separater Einzel-Server).
- Der Verwaltungsdienst ist mit der Verwaltungsverlaufsdatenbank auf dem Hauptdatenbankserver verbunden (Standardmäßig ist die Verwaltungsverlaufsdatenbank mit der Konfigurationsdatenbank identisch).
- Für die Datenbank des Verwaltungsverlaufs wurde keine Replikation eingerichtet (der Datenbankserver fungiert in Bezug auf die Quest One ActiveRoles-Replikation als separater Einzel-Server).

Unter diesen Bedingungen kann der Verwaltungsdienst angewiesen werden, bei einem Wechsel der Datenbankserverfunktion automatisch eine Verbindung zur neuen Hauptdatenbank herzustellen. Fügen Sie auf dem Computer, auf dem der Verwaltungsdienst ausgeführt wird, einen Zeichenkettenwert zu jedem dieser beiden Registrierungsschlüssel hinzu und starten Sie dann den Verwaltungsdienst neu:

- **Schlüssel:**
  HKLM\SOFTWARE\Aelita\Enterprise Directory Manager\DatabaseConnectionString\
  Wertname: Failover Partner
  Wertdaten: *<Gibt die SQL Server-Instanz an, die aktuell die Spiegelserverfunktion für die Konfigurationsdatenbank inne hat.>*
- **Schlüssel:**
  HKLM\SOFTWARE\Aelita\Enterprise Directory Manager\CHDatabaseConnectionString\
  Wertname: Failover Partner
  Wertdaten: *<Gibt die SQL Server-Instanz an, die aktuell die Spiegelserverfunktion für die Verwaltungsverlaufsdatenbank inne hat.>*

Wenn die Standardinstanz verwendet wird, sind die Wertdaten der NetBIOS-Name des Computers, der SQL Server ausführt. Andernfalls sind die Wertdaten der NetBIOS-Name des Computers, gefolgt von einem umgekehrten Schrägstrich, gefolgt vom Namen der Instanz (wie etwa *Computername**Instanzname*).

Standardmäßig wird dieselbe Datenbank für die Konfigurations- und Verwaltungsverlaufsdaten verwendet; daher sind die Wertdaten in den Schlüsseln „DatabaseConnectionString" und „CHDatabaseConnectionString" identisch.

In der Programmsteuerung von Quest One ActiveRoles kann der Spiegelungsstatus der von den einzelnen Instanzen des Verwaltungsdienstes verwendeten Datenbanken für die Einrichtungseinstellungen oder den Verwaltungsverlauf angezeigt werden:

1. Wählen Sie in der Konsolenstruktur **Configuration | Server Configuration | Administration Services**.
2. Doppelklicken Sie im Bereich „Details" auf den Namen des Verwaltungsdienstes, dessen Datenbank Sie untersuchen möchten.

3. Klicken Sie im Dialogfeld „Eigenschaften" auf die Registerkarte **Konfigurationsdatenbank** oder **Verwaltungsverlaufsdatenbank** und lesen Sie die Informationen im Bereich **Datenbankspiegelung**:
   - **Funktion.** Aktuelle Funktion der Datenbank in der Datenbankspiegelungssitzung (Hauptdatenbank oder gespiegelte Datenbank).
   - **Partner.** Der Instanzname und Computername für den anderen Partner in der Datenbankspiegelungssitzung.
   - **Status.** Aktueller Status der gespiegelten Datenbank und der Datenbankspiegelungssitzung. Weitere Angaben zu diesem Thema bietet der Punkt „Spiegelungsstatus" unter http://msdn.microsoft.com/en-us/library/ms189284.aspx

   Wenn keine Informationen im Bereich **Datenbankspiegelung** angezeigt werden, dann ist die Datenbankspiegelung nicht konfiguriert.

Sie können den Spiegelungsstatus einer Konfigurationsdatenbank oder einer Verwaltungsverlaufsdatenbank auch auf der Registerkarte **Allgemein** im Dialogfeld **Eigenschaften** für das Objekt anzeigen, das die Datenbank im Container **Configuration/Server Configuration/ Configuration Databases** bzw. **Configuration/Server Configuration/Management History Databases** angibt.

Erstellen und Verwenden virtueller Attribute

Quest One ActiveRoles bietet die Möglichkeit, zu jeder vorhandenen Art von Objekten selbst definierte (virtuelle) Attribute festzulegen. So können Sie zusätzliche Objekteigenschaften angeben, ohne das Active Directory-Schema zu erweitern. Beispielsweise können benutzerdefinierte Attribute verwendet werden, um bestimmte Benutzerdaten zu speichern.

Es können virtuelle Attribute eingerichtet werden, um die Attributwerte in der Quest One ActiveRoles-Datenbank zu speichern. Ansonsten müssen Sie für die Verwendung des virtuellen Attributs eine Skriptrichtlinie implementieren, die den Attributwert verarbeitet.

So erstellen Sie ein virtuelles Attribut:

1. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Server Configuration**.
2. Klicken Sie unter **Server Configuration** mit der rechten Maustaste auf **Virtual Attributes** und wählen Sie **Neu | Virtuelles Attribut** aus.
3. Folgen Sie den Anweisungen des Assistenten zum Hinzufügen eines virtuellen Attributs.
4. Geben Sie in die Felder **Allgemeiner Name** und **LDAP-Anzeigename** einen allgemeinen Namen und einen LDAP-Anzeigenamen für das neue Attribut ein.

   *Im Feld **Eindeutige X.500 Objekt-ID** können Sie optional den Standardwert der Eigenschaft „attributeID" (OID) für das neue Attribut ändern. Der Standardwert wird automatisch generiert. Wenn Sie einen eigenen Wert generieren möchten, können Sie das Tool Oidgen (oidgen.exe) im Windows Server Resource Kit verwenden.*

   *Im Feld **Schemakennungs-GUID** können Sie optional den Standardwert der Eigenschaft „schemaIDGUID" ändern. Der Standardwert wird automatisch generiert. Wenn das neue Attribut einen festen Wert für die Eigenschaft „schemaIDGUID" haben soll, ersetzen Sie den Standardwert durch den gewünschten Wert. Beispielsweise können Sie die GUID mit dem Tool Uuidgen im Microsoft Platform SDK generieren.*

5. Optional können Sie in das Feld **Beschreibung** eine Beschreibung für das neue virtuelle Attribut eingeben. Klicken Sie auf **Weiter**.

6. Klicken Sie in der Liste **Syntax** auf die gewünschte Syntax für das neue virtuelle Attribut. Wenn das neue Attribut mehrwertig sein soll, aktivieren Sie das Kontrollkästchen **Mehrere Werte**. Klicken Sie auf **Weiter**.
7. Aktivieren Sie die Kontrollkästchen neben den Objektklassen, denen Sie das virtuelle Attribut zuordnen möchten. Klicken Sie auf **Weiter**.

   *Wenn Sie das neue Attribut Objektklassen zuordnen möchten, die nicht standardmäßig aufgelistet sind, aktivieren Sie das Kontrollkästchen **Alle mögliche Klassen anzeigen**.*
8. Wenn die Werte eines Attributes in der Quest One ActiveRoles-Datenbank gespeichert werden sollen, setzen Sie auf der Seite des **Attributspeichers** einen Haken in das entsprechende Kästchen.

   Wenn Sie die Attributwerte nicht in der Datenbank speichern möchten, ist eine Skriptrichtlinie erforderlich, die beim Abrufen des Attributs den Attributwert bereitstellt und beim Aktualisieren des Attributs den Attributwert speichert.

   Sie sollten diese Option jedoch mit Bedacht verwenden. Die Speicherung der Attributwerte in der Einrichtungseinstellungendatenbank von Quest One ActiveRoles kann den Umfang der Datenbank erheblich erhöhen.

   Diese Option kann nach der Erstellung des Attributs mit Hilfe der Verwaltungsfunktionen für Eigenschaften des virtuellen Attributs geändert werden.
9. Klicken Sie auf **Weiter** und klicken Sie dann auf **Fertig stellen**, um den Assistenten abzuschließen.

Stellen Sie nach dem Hinzufügen des neuen virtuellen Attributs erneut eine Verbindung mit dem Verwaltungsdienst her. Das neue virtuelle Attribut wird im Container **Virtual Attributes** unter **Configuration/Server Configuration** angezeigt.

Gehen Sie folgendermaßen vor, um den Wert eines virtuellen Attributs für ein Objekt anzuzeigen oder zu ändern:

1. Klicken Sie mit der rechten Maustaste auf das Objekt und wählen Sie **Alle Aufgaben | Erweiterte Eigenschaften** aus.
2. Aktivieren Sie die Kontrollkästchen **Alle möglichen Attribute anzeigen** und **Attribute mit leeren Werten einschließen**, damit in der Liste im Dialogfeld **Erweiterte Eigenschaften** alle Attribute des Objekts angezeigt werden.
3. Klicken Sie auf das Attribut in der Liste und klicken Sie dann auf die Schaltfläche unter der Liste.
4. Zeigen Sie in dem sich öffnenden Dialogfeld den Wert des Attributs an oder ändern Sie ihn.

Weitere Informationen zu den virtuellen Attributen bietet das SDK zu Quest One ActiveRoles.

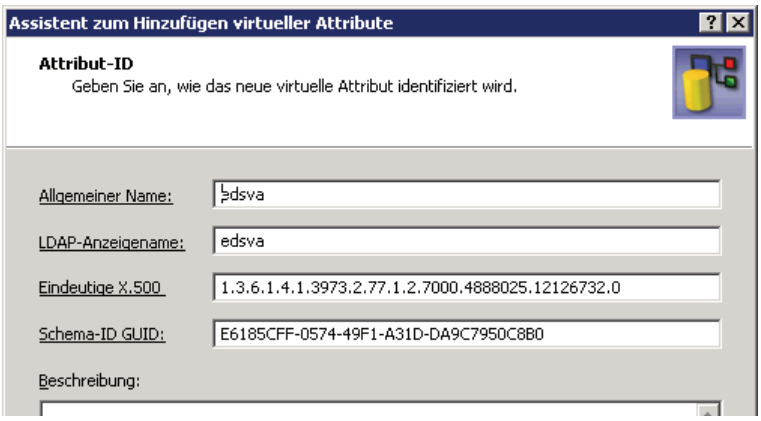
Szenario: Implementieren eines Attributs für den Geburtstag

In diesem Szenario wird veranschaulicht, wie Sie ein virtuelles Attribut erstellen und verwenden, um Informationen zu den Geburtstagen der Benutzer zu speichern.

So erstellen Sie das Attribut für den Geburtstag:

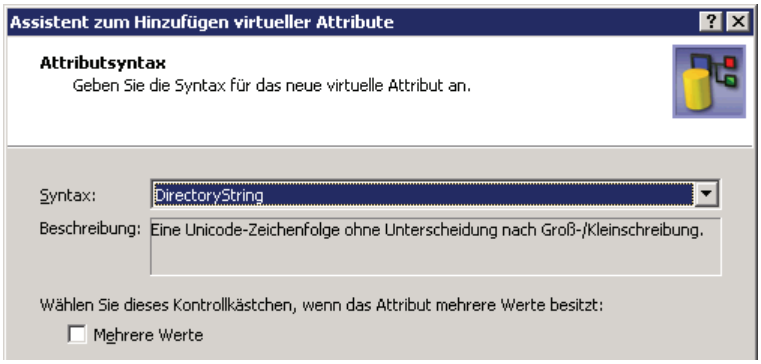
1. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Server Configuration**.
2. Klicken Sie unter **Server Configuration** mit der rechten Maustaste auf **Virtual Attributes** und wählen Sie **Neu | Virtuelles Attribut** aus.
3. Klicken Sie auf **Weiter**.

4. Geben Sie in die Felder **Allgemeiner Name** und **LDAP-Anzeigename** jeweils den Wert **Geburtstag** ein, wie in der folgenden Abbildung gezeigt.

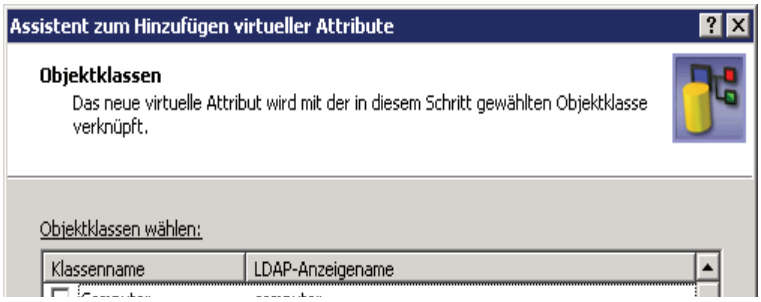


5. Klicken Sie auf **Weiter**.

   *Die Seite **Attributsyntax** sollte nun der folgenden Abbildung entsprechen.*


Assistent zum Hinzufügen virtueller Attribute
Attributsyntax
Geben Sie die Syntax für das neue virtuelle Attribut an.
Syntax:
DirectoryString
Beschreibung:
Eine Unicode-Zeichenfolge ohne Unterscheidung nach Groß-/Kleinschreibung.
Wählen Sie dieses Kontrollkästchen, wenn das Attribut mehrere Werte besitzt:
Mehrere Werte

6. Klicken Sie auf **Weiter**.
7. Aktivieren Sie auf der Seite **Objektklassen** das Kontrollkästchen neben **Benutzer**, wie in der folgenden Abbildung gezeigt.



8. Klicken Sie auf **Weiter**.
9. Aktivieren Sie im Fenster für die Attributspeicherung das Kontrollkästchen **Werte dieses virtuellen Attributs in der ActiveRoles Verwaltungsdatenbank speichern**.
10. Klicken Sie auf **Weiter** und klicken Sie dann auf **Fertig stellen**, um den Assistenten abzuschließen.

Stellen Sie zum Aktivieren des neuen Attributs wie folgt erneut eine Verbindung mit dem Verwaltungsdienst her: Klicken Sie mit der rechten Maustaste auf den Stamm der Konsolenstruktur und klicken Sie dann auf **Erneut verbinden**.

In der Programmsteuerung von Quest One ActiveRoles kann das Attribut **Geburtstag** in einem Benutzerkonto folgendermaßen verwaltet werden:

1. Klicken Sie mit der rechten Maustaste auf das Benutzerkonto und wählen Sie dann **Alle Aufgaben | Erweiterte Eigenschaften**.
2. Aktivieren Sie im Dialogfeld **Erweiterte Eigenschaften** die Kontrollkästchen **Alle möglichen Attribute anzeigen** und **Attribute mit leeren Werten einschließen**.
3. Klicken Sie in der Liste der Eigenschaften auf **Geburtstag** und klicken Sie dann auf **Bearbeiten.**
4. Geben Sie in das Feld **Wert** einen Geburtstag ein.
5. Klicken Sie auf **OK**.

Das Attribut **Geburtstag** kann auch über die Web-Schnittstelle von Quest One ActiveRoles verwaltet werden.

Fügen Sie zunächst das Feld **Geburtsdatum** dem Formular hinzu, auf dem Benutzereigenschaften angezeigt werden, und ordnen Sie dieses Feld dann dem Attribut **Geburtsdatum** zu. Um dies zu erreichen, passen Sie das Formular an. Anleitungen zum Hinzufügen von Formularfeldern bietet der Administratorenleifaden für *Quest One ActiveRoles-Web-Schnittstellen*.

Das Attribut **Geburtstag** kann dann verwaltet werden, indem Personen auf einer Seite des Web-Interface auf Benutzereigenschaften zugreifen. Benutzer können dieses Attribut zum Beispiel über die Site für die Selbstverwaltung anzeigen und ändern, vorausgesetzt, dass die Selbstverwaltung implementiert ist (siehe Szenario 2: Implementieren der Selbstverwaltung im Kapitel Rollenbasierte Administration weiter oben in diesem Dokument).

Untersuchen von Client-Sitzungen

In der Programmsteuerung von Quest One ActiveRoles werden umfangreiche Angaben zu den Verbindungen mit Client-Rechnern angezeigt. Wenn die Konsole eine Verbindung mit einem bestimmten Verwaltungsdienst aufweist, können Sie untersuchen, welche Clients diesen Dienst verwenden. Folgende Sitzungsinformationen werden auf der Konsole bereitgestellt:

- **Benutzer.** Anmeldename des Kontos, mit dem die Sitzung eine Verbindung mit dem Verwaltungsdienst herstellt.
- **ActiveRoles Admin.** Hier wird angezeigt, ob der Client als Mitglied des Administratorenkontos von ActiveRoles angemeldet ist, und somit über Administratorrechte in Bezug auf den Verwaltungsdienst verfügt, oder nicht.
- **Clientversion.** Clientanwendung, z.B. MMC-Benutzeroberfläche oder Web-Interface, und ihre Version.
- **Letzter Zugriff.** Datum und Uhrzeit des letzten Zugriffs auf den Verwaltungsdienst in dieser Sitzung.
- **Anmeldezeit.** Datum und Uhrzeit, zu denen die Sitzung geöffnet wurde.
- **Clienthost.** DNS-Name (Domain Name System) des Computers, auf dem die Clientanwendung ausgeführt wird.
- **Clientsite.** Netzwerk-Site des Computers, auf dem die Clientanwendung ausgeführt wird.

Gehen Sie folgendermaßen vor, um eine Liste von Client-Sitzungen für den Verwaltungsdienst anzuzeigen:

1. Stellen Sie eine Verbindung zu dem Verwaltungsdienst her, dessen Client-Sitzungen Sie untersuchen möchten.
2. Erweitern Sie in der Konsolenstruktur den Eintrag **Configuration | Server Configuration** und wählen Sie dann **Client Sessions**.

   Daraufhin werden im Bereich „Details" die Client-Sitzungen für den Verwaltungsdienst aufgeführt, mit dem die Konsole verbunden ist.

Mit dem Kontextmenü für eine Clientsitzung können Sie auch folgende Aufgaben ausführen:

- Senden von E-Mail an den Sitzungsbenutzer.
- Trennen der Sitzung vom Verwaltungsdienst.
- Anzeigen zusätzlicher Informationen zur Sitzung.

Um beispielsweise zusätzliche Informationen zu einer Sitzung anzuzeigen, klicken Sie im Bereich „Details" mit der rechten Maustaste auf die Sitzung und klicken Sie dann auf **Eigenschaften**.

Das Dialogfeld **Eigenschaften** für eine Client-Sitzung umfasst die folgenden Registerkarten:

- **Allgemein.** Informationen zum Sitzungsbenutzer, zur Clientversion, zum Clienthost und zur Clientsite.
- **Clientaktivität.** Informationen zum Zeitpunkt der Anmeldung, zum Zeitpunkt des letzten Zugriffs sowie zur Anzahl der in der Sitzung ausgeführten Vorgänge, gruppiert nach Vorgangstyp.
- **Mitglied von.** Liste aller Sicherheitsgruppen, die aufgrund eines transitiven Erweiterungsvorgangs für die Gruppenmitgliedschaft für den Sitzungsbenutzer zum Zeitpunkt des Sitzungsbeginns berechnet wurden.
- **Domänencontroller.** Informationen zu den Domänencontrollern, mit denen Verzeichnisdaten innerhalb der Sitzung abgerufen und aktualisiert werden.

Überwachen der Leistung

Quest One ActiveRoles beinhaltet eine Reihe von Leistungsindikatoren zur Überwachung unterschiedlicher Aspekte der Leistungsfähigkeit des Verwaltungsdienstes. Die Leistungsindikatoren sind in folgenden Leistungsobjekten gruppiert:

- **Anforderungen.** Zählt Datenverwaltungsanforderungen, die an den Verwaltungsdienst übermittelt werden.
- **LDAP-Vorgänge.** Zählt LDAP-Anforderungen, die vom Verwaltungsdienst ausgegeben werden.
- **Berechtigungsweitergabe.** Zählt Änderungen an der Active Directory-Sicherheit, die vom Verwaltungsdienst vorgenommen werden.
- **Externe Änderungen.** Zählt Datenänderungen, die der Verwaltungsdienst aus Active Directory abruft, sowie Änderungen, die an der Verwaltungsdatenbank vorgenommen werden.
- **Skriptmodule.** Erfasst werden die durchschnittliche Ausführungszeit der Skriptmodule von Quest One ActiveRoles, die Häufigkeit, mit der die einzelnen Skriptmodule ausgeführt wurden, sowie die Anzahl der Skriptmodulinstanzen, die zu dem gegebenen Zeitpunkt ausgeführt werden.
- **Verschiedenes.** Zählt die Anzahl der mit dem Verwaltungsdienst verbundenen Clients und die Anzahl der in der Warteschlange befindlichen Post-Richtlinienverarbeitungsvorgänge.

Um die Leistungsindikatoren des Verwaltungsdienstes zu untersuchen, können Sie das Tool „Leistung" auf dem Computer mit dem Verwaltungsdienst verwenden:

1. So öffnen Sie das Tool „Leistung": Klicken Sie auf **Starten** und wählen Sie **Alle Programme | Administrative Tools | Leistung**.
2. Wählen Sie in der Konsolenstruktur **Systemmonitor** aus.
3. Klicken Sie im Bereich „Details", und drücken Sie dann STRG+I, um das Dialogfeld **Zähler hinzufügen** anzuzeigen.
4. Wählen Sie in der Liste im Feld **Leistungsobjekt** einen beliebigen Namen aus, der mit dem Präfix **AR Server** beginnt. Sie können beispielsweise **AR Server:Anforderungen** auswählen.
5. Wählen Sie in der Liste der Leistungsindikatoren einen Eintrag aus. Sie können beispielsweise **Anforderungen/Sek**. auswählen.
6. Klicken Sie auf **Hinzufügen** und dann auf **Schließen**

Nun zeigt das Tool „Leistung" die Ausgabe des ausgewählten Leistungsindikators an.

Anpassen der Konsole

Die Programmsteuerung von Quest One ActiveRoles bietet eine unkomplizierte Möglichkeit, die in der Programmsteuerung zu findenden Assistenten zur Erstellung von Objekten sowie die Eigenschaftsseiten selbst zu gestalten und die angezeigten Bezeichnungen der Objektarten und -eigenschaften individuell anzupassen. Die Individualisierung erfolgt mittels Active Directory-Objekten, die als *Anzeigebezeichner* bezeichnet werden.

Jedes Anzeigebezeichnerobjekt enthält Informationen, die die verschiedenen Benutzerschnittstellenelemente für einen bestimmten Objekttyp beschreiben. Diese Elemente umfassen (sind jedoch nicht beschränkt darauf) die Seiten des Erstellungsassistenten, die Eigenschaftenseiten und Namen, die für Objekttypen und Eigenschaften in Benutzerschnittstellen verwendet werden.

In den folgenden Abschnitten sind die mit der Individualisierung zusammenhängenden Funktionsmerkmale beschrieben, die auf der Verwendung von Anzeigebezeichner basieren:

- **Seite Andere Eigenschaften** im Objekterstellungsassistenten
- **Registerkarte Andere Eigenschaften** im Dialogfeld **Eigenschaften**
- Anpassen von Anzeigenamen

Seite „Andere Eigenschaften" im Objekterstellungsassistent

In der Quest One ActiveRoles-Programmsteuerung werden Verzeichnisobjekte unter Verwendung von Erstellungsassistenten angelegt. Die Erstellung eines Benutzerkontos startet den Assistenten „Neues Objekt – Benutzer". Die Programmsteuerung von Quest One ActiveRoles ermöglicht die Erweiterung der Erstellungsassistenten um eine zusätzliche Seite, auf der im Verlauf des Objekterstellungsvorgangs Eintrage zu ergänzenden Eigenschaften vorgenommen werden können.

Die Quest One ActiveRoles-Programmsteuerung erleichtert die Anzeige oder Änderung des Eigenschaftenbundels auf der zusätzlichen Seite des Assistenten durch den Einsatz einer gesonderten Registerkarte für die Anzeigebezeichnerobjekte (Display Specifier Objects) im Dialogfeld **Eigenschaften**. Die Registerkarte **Andere anzuzeigende Eigenschaften** bietet die Möglichkeit zur

Anpassung der auf der Erweiterungsseite der Assistenten zur Objekterstellung enthaltenen Eigenschaften. Wenn keine Eigenschaften für die Aufnahme in die Erweiterungsseite vorhanden sind, wird die Seite nicht angezeigt.

Die Registerkarte **Andere anzuzeigende Eigenschaften** kann verwendet werden, um Eigenschaften zur Erweiterungsseite des Erstellungsassistenten für den Objekttyp, mit dem der Anzeigebezeichner verbunden ist, hinzuzufügen bzw. von ihr zu entfernen. Auf der Registerkarte sind die Objekteigenschaften aufgeführt, die auf der Erweiterungsseite enthalten sind. Sie ermöglicht Ihnen, Änderungen an dieser Liste vorzunehmen.

Gehen Sie wie nachfolgend beschrieben vor, um die Seite **Andere Eigenschaften** zum Assistenten „Neues Objekt – Benutzer" hinzuzufügen. Ebenso können Sie den Erstellungsassistent für einen anderen Objekttyp erweitern, indem Sie einen benutzerdefinierten Anzeigebezeichner für diesen Objekttyp erstellen und konfigurieren. Um zum Beispiel den Assistenten für Gruppen, Computer oder Organisationseinheiten zu erweitern, erstellen und konfigurieren Sie einen benutzerdefinierten Anzeigebezeichner mit dem Namen **Gruppe-Anzeige**, **Computeranzeige** bzw. **Organisationseinheit-Anzeige**.

Beachten Sie, dass bei den Namen der Anzeigebezeichner zwischen Groß- und Kleinschreibung unterschieden wird. Sie müssen den Namen daher genau so eingeben, wie er im Active Directory Schema angegeben ist. Um die Namen der Anzeigebezeichner anzuzeigen, können Sie die Konsole verwenden, um den Container „Active Directory | Configuration Container | Display Specifiers | 409" im Rohansichtsmodus zu untersuchen.

Gehen Sie folgendermaßen vor, um den Assistenten „Neues Objekt – Benutzer" zu erweitern:

1. Wechseln Sie nach dem Öffnen der Programmsteuerung von Quest One ActiveRoles in den Originalansichtsmodus (klicken Sie auf **Ansicht | Modus** und dann auf **Original**, klicken Sie anschließend auf **OK**).
2. Klappen Sie im Baum des Programmsteuerung **Einrichtungseinstellungen | Anwendungseinstellungen** auf und klicken Sie auf den Container mit der Bezeichnung **ActiveRoles-Anzeigebezeichner (vom Benutzer erstellt)**.
3. Durch Verwendung des Befehls **Alle Vorgange | Erweiterte Erstellung** kann der entsprechende lokale Container angelegt werden.

   *Der benutzerdefinierte Anzeigebezeichner muss in dem lokalen Container erstellt werden, der mit dem lokalen Container Ihrer Umgebung übereinstimmt. Diese lokalen Container werden mit Hilfe der hexadezimalen Darstellung der LCID dieser lokalen Container benannt. Folglich heißt der US-amerikanische/englische lokale Container **409**, der deutsche lokale Container **407**, der japanische lokale Container **411** usw.*

   *Möglicherweise muss dieser lokale Container zuerst angelegt werden. Verwenden Sie hierzu den Befehl **Alle Aufgaben | Erweiterte Erstellung**, um ein Objekt der Klasse **EDS-Anzeigebezeichner-Container** zu erstellen.*

4. Erstellen Sie im lokalen Container den benutzerdefinierten Anzeigebezeichner mit dem Namen **Benutzer-Anzeige**.

   *Verwenden Sie hierzu den Befehl **Alle Aufgaben | Erweiterte Erstellung** für den lokalen Container, um ein Objekt der Klasse **Anzeigebezeichner** zu erstellen. Beachten Sie, dass beim Namen des Anzeigebezeichners zwischen Groß- und Kleinschreibung unterschieden wird. Daher sollten Sie den Namen für den neuen Anzeigebezeichner genau als **Benutzer-Anzeige** und nicht als Benutzeranzeige oder BenutzerAnzeige eingeben.*

5. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf **Benutzer-Anzeige** und klicken Sie dann auf **Eigenschaften**.
6. Rufen Sie die Registerkarte **Andere anzuzeigende Eigenschaften** auf.

7. Fügen Sie eine oder mehrere Eigenschaften zur Liste **Andere Eigenschaften bei der Objekterstellung** hinzu. Klicken Sie dann auf **OK**.
8. Starten Sie den Verwaltungsdienst neu und stellen Sie dann erneut die Verbindung zwischen der Konsole und dem Dienst her, damit die Änderungen wirksam werden.

Infolge dieser Maßnahmen enthalt der „Neues Objekt - Benutzer"-Assistent eine zusätzliche Seite, auf der die Werte für die in Schritt 7 ausgewählten Eigenschaften angeben werden können. Der Assistent kann in der Programmsteuerung von Quest One ActiveRoles durch Anklicken einer Organisationseinheit in dem Baum der Programmsteuerung mit der rechten Maustaste und einen anschließenden Linksklick auf **Neu | Benutzer** aufgerufen werden. Folgen Sie den Anweisungen des Assistenten, um die Seite aufzurufen, die die Liste der „Sonstigen" Eigenschaften enthält.

Registerkarte „Andere Eigenschaften" im Dialogfeld „Eigenschaften"

Die Programmsteuerung von Quest One ActiveRoles ermöglicht darüber hinaus die Erweiterung des **Eigenschaften**-Dialogfeldes um die Aufnahme von Verzeichnisobjekten durch eine zusätzliche Registerkarte mit der Bezeichnung **Weitere Eigenschaften**, wodurch die Verwaltung eines selbst festgelegten Bündels von Objekteigenschaften mithilfe des Befehls **Eigenschaften** vorgenommen werden kann.

Die Programmsteuerung von Quest One ActiveRoles erleichtert die Anzeige und Änderung des Eigenschaftenbündels unter der Registerkarte **Weitere Eigenschaften** durch die Verwendung einer gesonderten Registerkarte für die Anzeigebezeichnerobjekte (Display Specifier Objects) im Dialogfeld **Eigenschaften**. Auf diese Weise können Sie die Reihe der auf der Registerkarte **Andere Eigenschaften enthaltenen Eigenschaften** anpassen. Beachten Sie, dass das Dialogfeld **Eigenschaften** die Registerkarte **Andere Eigenschaften** nur dann enthält, wenn anzuzeigende Eigenschaften auf dieser Registerkarte vorhanden sind.

Die Registerkarte **Andere anzuzeigende Eigenschaften** kann verwendet werden, um Eigenschaften zur Registerkarte **Andere Eigenschaften** hinzuzufügen bzw. von ihr zu entfernen, die nur den Objekttyp betreffen, mit dem der Anzeigebezeichner verbunden ist. Auf der Registerkarte **Andere anzuzeigende Eigenschaften** sind die Objekteigenschaften aufgeführt, die auf der Registerkarte **Andere Eigenschaften** für den Objekttyp enthalten sind. Sie ermöglicht Ihnen, Änderungen an dieser Liste vorzunehmen.

Gehen Sie wie nachfolgend beschrieben vor, um die Registerkarte **Andere Eigenschaften** zum Dialogfeld **Eigenschaften** für Benutzerobjekte hinzuzufügen. Ebenso können Sie die Eigenschaftenseiten für einen anderen Objekttyp erweitern, indem Sie einen benutzerdefinierten Anzeigebezeichner für diesen Objekttyp erstellen und konfigurieren. Um zum Beispiel das Dialogfeld **Eigenschaften** für Gruppen, Computer oder Organisationseinheiten zu erweitern, erstellen und konfigurieren Sie einen benutzerdefinierten Anzeigebezeichner mit dem Namen **Gruppe-Anzeige**, **Computeranzeige** bzw. **Organisationseinheit-Anzeige**.

Beachten Sie, dass bei den Namen der Anzeigebezeichner zwischen Groß- und Kleinschreibung unterschieden wird. Sie müssen den Namen daher genau so eingeben, wie er im Active Directory Schema angegeben ist. Um die Namen der Anzeigebezeichner anzuzeigen, können Sie die Konsole verwenden, um den Container „Active Directory | Configuration Container | Display Specifiers | 409" im Rohansichtsmodus zu untersuchen.

Gehen Sie folgendermaßen vor, um das Dialogfeld „Eigenschaften" für Benutzerobjekte zu erweitern:

1. Wechseln Sie nach dem Öffnen der Programmsteuerung von Quest One ActiveRoles in den Originalansichtsmodus (klicken Sie auf **Ansicht | Modus** und dann auf **Original**, klicken Sie anschließend auf **OK**).
2. Klappen Sie im Baum des Programmsteuerung **Einrichtungseinstellungen | Anwendungseinstellungen** auf und klicken Sie auf den Container mit der Bezeichnung **ActiveRoles-Anzeigebezeichner (vom Benutzer erstellt)**.
3. Durch Verwendung des Befehls **Alle Vorgange | Erweiterte Erstellung** kann der entsprechende lokale Container angelegt werden.

   *Der benutzerdefinierte Anzeigebezeichner muss in dem lokalen Container erstellt werden, der mit dem lokalen Container Ihrer Umgebung übereinstimmt. Diese lokalen Container werden mit Hilfe der hexadezimalen Darstellung der LCID dieser lokalen Container benannt. Folglich heißt der US-amerikanische/englische lokale Container **409**, der deutsche lokale Container **407**, der japanische lokale Container **411** usw.*

   *Möglicherweise muss dieser lokale Container zuerst angelegt werden. Verwenden Sie hierzu den Befehl **Alle Aufgaben | Erweiterte Erstellung**, um ein Objekt der Klasse **EDS-Anzeigebezeichner-Container** zu erstellen.*

4. Erstellen Sie im lokalen Container den benutzerdefinierten Anzeigebezeichner mit dem Namen **Benutzer-Anzeige**.

   *Verwenden Sie hierzu den Befehl **Alle Aufgaben | Erweiterte Erstellung** für den lokalen Container, um ein Objekt der Klasse **Anzeigebezeichner** zu erstellen. Beachten Sie, dass beim Namen des Anzeigebezeichners zwischen Groß- und Kleinschreibung unterschieden wird. Daher sollten Sie den Namen für den neuen Anzeigebezeichner genau als **Benutzer-Anzeige** und nicht als Benutzeranzeige oder BenutzerAnzeige eingeben.*

5. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf **Benutzer-Anzeige** und klicken Sie dann auf **Eigenschaften**.
6. Rufen Sie die Registerkarte **Andere anzuzeigende Eigenschaften** auf.
7. Fügen Sie eine oder mehrere Eigenschaften zur Liste **Andere Eigenschaften auf den Objekteigenschaftsseiten** hinzu. Klicken Sie dann auf **OK**.
8. Starten Sie den Verwaltungsdienst neu und stellen Sie dann erneut die Verbindung zwischen der Konsole und dem Dienst her, damit die Änderungen wirksam werden.

Infolge dieser Maßnahmen enthalt das **Eigenschaften**-Dialogfeld die Registerkarte **Weitere Eigenschaften**, in der die Werte der in Schritt 7 ausgewählten Eigenschaften angezeigt oder geändert werden können. Der Zugriff auf diese Registerkarte erfolgt in der Programmsteuerung von Quest One ActiveRoles durch einen Rechtsklick auf ein Benutzerkonto und einen anschließenden Klick mit der linken Maustaste auf **Eigenschaften**.

Anpassen von Anzeigenamen

In Active Directory kann jeder Objekttyp über einen Anzeigenamen verfügen, und jede Eigenschaft eines Objekts kann ebenfalls einen Anzeigenamen haben. In Benutzerschnittstellen werden Anzeigenamen als benutzerfreundliche Namen verwendet, um die Identifikation von Objekttypen und -eigenschaften zu erleichtern. Die Anzeigenamen für einen bestimmten Objekttyp werden in den Anzeigebezeichnerobjekten für den entsprechenden Objekttyp gespeichert.

Die Quest One ActiveRoles-Programmsteuerung erleichtert die Anzeige oder Änderung der angezeigten Namen dank einer gesonderten Registerkarte für die Anzeigebezeichnerobjekte (Display Specifier Objects) im Dialogfeld **Eigenschaften**. Die Registerkarte **Anzeigenamen** bietet eine benutzerfreundliche Methode zur Anpassung von Anzeigenamen für Objekttypen und eigenschaften.

Die Registerkarte **Anzeigenamen** kann verwendet werden, um den Anzeigenamen für den Objekttyp, mit dem der Anzeigebezeichner verbunden ist, anzugeben oder zu ändern und um Anzeigenamen für die Eigenschaften von Objekten dieses Typs hinzuzufügen, zu ändern oder zu entfernen. Die Eigenschafts-Anzeigenamen werden mit Hilfe einer Liste von Namenspaaren verwaltet, wobei der erste Name der LDAP-Anzeigename einer Eigenschaft, gefolgt vom Anzeigenamen dieser Eigenschaft ist.

Gehen Sie folgendermaßen vor, um den englischsprachigen Anzeigenamen für die Klasse „Benutzerobjekt" innerhalb einer Gesamtstruktur zu ändern:

1. Wechseln Sie nach dem Öffnen der Programmsteuerung von Quest One ActiveRoles in den Originalansichtsmodus (klicken Sie auf **Ansicht | Modus** und dann auf **Original**, klicken Sie anschließend auf **OK**).
2. Erweitern Sie in der Konsolenstruktur den Eintrag **Active Directory | Configuration Container | Display Specifiers** und wählen Sie den Container **409** aus.
3. Klicken Sie im Bereich „Details" mit der rechten Maustaste auf **Benutzer-Anzeige** und klicken Sie dann auf **Eigenschaften**.
4. Ändern Sie auf der Registerkarte **Anzeigenamen** unter **Anzeigename für Objekttyp** den Anzeigenamen und klicken Sie dann auf **OK**.
5. Starten Sie den Verwaltungsdienst neu und stellen Sie dann erneut die Verbindung zwischen der Konsole und dem Dienst her, damit die Änderungen wirksam werden.

Durch die Ausführung dieser Schritte werden Änderungen an dem in Active Directory vorgehaltenen Anzeigebezeichner vor, weswegen die von Ihnen vorgenommenen Änderungen nicht nur Quest One ActiveRoles betreffen, sondern auch alle Client-Anwendungen, die dazu dienen, Benutzerobjekte in Active Directory zu verwalten, beispielsweise Benutzer oder Computer unter Active Directory. Wenn die angezeigten Namen lediglich innerhalb der Client-Schnittstellen von Quest One ActiveRoles individuell gestaltet werden sollen, müssen die entsprechenden Änderungen an den in dem Container für die **ActiveRoles-Anzeigebezeichner (vom Benutzer erstellt)** enthaltenen selbst erstellten Anzeigebezeichnern vorgenommen werden. Das Dialogfeld **Eigenschaften** für benutzerdefinierte Anzeigebezeichner umfasst auch die Registerkarte **Anzeigenamen**, die es Ihnen ermöglicht, die Anzeigenamen so anzupassen, dass Ihre Änderungen nur die Quest One ActiveRoles-Umgebung betreffen.

Änderung des Administratorenkontos für ActiveRoles

Bei der Installation des Verwaltungsdienstes von ActiveRoles werden Sie zur Angabe des Gruppen- oder Benutzerkontos aufgefordert, das über die vollständigen Zugriffsrechte auf die Einrichtungseinstellungen und Daten von ActiveRoles haben soll. Dieses Konto wird als Administrator von ActiveRoles oder kurz als ActiveRoles-Admin bezeichnet. Standardmäßig ist ActiveRoles Admin die lokale Verwaltergruppe auf dem Rechner, der den Verwaltungsdienst ausführt. Sie können diese Einstellung wahrend der Installation des Verwaltungsdienstes in dem Assistenten für die Ersteinrichtung ändern. Nach der Installation des Verwaltungsdienstes kann durch entsprechende Bearbeitung des Registrierungsverzeichnisses auf dem Computer, auf dem der Verwaltungsdienst installiert ist, ein anderes Administratorenkonto für ActiveRoles gewählt werden. Beachten Sie bitte, dass die Einstellung des ActiveRoles-Admin eine Besonderheit der Instanz des Verwaltungsdienstes ist. Wenn in einer Umgebung mehrere Verwaltungsdienstinstanzen eingerichtet sind, müssen die Änderungen an dem Registrierungsverzeichnis auf alle Computer angewendet werden, auf denen der Verwaltungsdienst lauft.

Öffnen Sie zur Änderung des Administratorenkontos für ActiveRoles

1. auf dem Computer, auf dem der Verwaltungsdienst lauft, das Hilfsprogramm Regedit und navigieren Sie zu dem Registrierungsverzeichnisschlussel **HKLM\SOFTWARE\Aelita\Enterprise Directory Manager**.
2. Ersetzen Sie die Daten des **DSAdministrators**-Wertes in diesem Schlüssel durch den Namen des Gruppen- oder Benutzerkontos, das Sie zum ActiveRoles-Admin machen mochten.

Sofern der ActiveRoles-Admin weder eine lokale Computergruppe noch ein lokaler Benutzer ist, muss der Name in dem **DSAdministrators**-Wert folgende Form aufweisen: <Domain-Name>\<Kontoname>; wobei der <Domain-Name> der NetBIOS-Name der Domain ist und der <Kontoname> der Vor-Windows 2000-Name (sAMAccountName) der Domain-Gruppe oder des Domain-Benutzers.

Der in dem Wert für die **DSAdministrators** angegebene Benutzer verfügt über die Administratorrechte in Bezug auf ActiveRoles. Ist in dem **DSAdministrators**-Wert eine Gruppe angegeben, so besitzt jedes Mitglied dieser Gruppe die Administratorrechte in Bezug auf ActiveRoles. Beachten Sie bitte, dass die Mitglieder der lokalen Administratorengruppe auf dem Rechner, auf dem der Verwaltungsdienst lauft, unabhängig von dem für die **DSAdministrators** eingestellten Wert über die Administratorrechte in Bezug auf ActiveRoles verfügen. Dieser Gruppe können die Administratorrechte in Bezug auf ActiveRoles nicht entzogen werden.

Das Programm zur Verbesserung der Software

Das Software-Verbesserungsprogramm von Quest® liefert der für das Produkt zuständigen Mannschaft verallgemeinerte Angaben dazu, wie das Produkt von den Kunden genutzt wird. Diese Angaben sowie die unmittelbaren Ruckmeldungen der Kunden durch die Kundenbetreuung und Foren helfen uns sicherzustellen, dass wir in der Lage sind, Ihre aktuellen und zukünftigen Wunsche zu erfüllen.

Wie geht das vonstatten?

Wenn Sie sich dazu entschließen, an dem Programm teilzunehmen, übertragt das Programm automatisch Ruckmeldungen an uns. Diese Daten werden auf Servern in den Vereinigten Staaten gesammelt und gespeichert.

Die Teilnahme an dem Programm ist freiwillig und Sie können sie jederzeit beenden.

Welche Informationen werden gesammelt?

Von uns werden ausschließlich erfasst:

- Angaben zu Ihrer Hard- und Software-Ausstattung: die interne und die externe IP-Adresse, die Versionen des Betriebssystems und von MS Exchange sowie Ihr Domain-Bestand und -Niveau.
- Angaben zu der Art Ihrer Nutzung der Funktionen von ActiveRoles: die Anzahl der verwalteten Einheiten, der dynamischen Gruppen, Gruppenfamilien, virtuellen Attribute, Richtlinienobjekte, Arbeitsablaufe, Skriptmodule usf.

Welche Auswirkungen hat das auf die Infrastruktur?

Wenn Sie sich entscheiden, an dem Programm zur Verbesserung der Software teilzunehmen:

- wird die Leistungsfähigkeit der Software nicht beeinträchtigt.
- Die Software erzeugt in sehr geringem Umfang zusätzlichen Datenverkehr im Internet, in der Regel nicht mehr als 0,1 kB / s.

Alle Funktionen dieser Software laufen unabhängig davon, ob Sie an dem Programm teilnehmen oder nicht.

Klicken Sie, um an dem Programm zur Verbesserung der Software teilzunehmen,

1. im Baum der Programmsteuerung von ActiveRoles mit der rechten Maustaste auf den Stammknoten und dann mit links auf das **Software-Verbesserungsprogramm**.
2. Klicken Sie in dem Dialogfeld, das eingeblendet wird, auf **Ja, ich bin bereit, an dem Programm zur Verbesserung der Software teilzunehmen.**

Klicken Sie, wenn Sie nicht oder nicht langer teilnehmen mochten, auf **Nein, ich mochte nicht an dem Programm zur Verbesserung der Software teilnehmen.**

16

Anhang

- Anhang A: Verwenden regulärer Ausdrücke
- Anhang B: Administrative Vorlage für ActiveRoles
- Anhang C: Ports für Datenübertragung

Anhang A: Verwenden regulärer Ausdrücke

Bei der Konfiguration der Suchfilterbedingungen oder Eigenschaftsüberprüfungskriterien müssen reguläre Ausdrücke verwendet werden. In diesem Abschnitt wird die Syntax für reguläre Ausdrücke erläutert.

Ein regulärer Ausdruck ist ein Textmuster, das aus gewöhnlichen Zeichen (z.B. den Buchstaben a bis z) und Sonderzeichen, den so genannten Metazeichen, besteht. Er dient als Vorlage, mit der die Übereinstimmung eines Musters aus Zeichen mit dem zu untersuchenden Zeichenfolgenwert überprüft wird.

Die folgende Tabelle enthält eine Liste von Metazeichen und ihrem Verhalten im Kontext regulärer Ausdrücke, mit denen Suchfilterbedingungen und Eigenschaftsüberprüfungskriterien in Quest One ActiveRoles erstellt werden können. Um bei einem Metazeichen eine Übereinstimmung mit dem Zeichen selbst zu suchen, stellen Sie ihm einen umgekehrten Schrägstrich (\) voran.

ZEICHEN	DEFINITION
****	Markiert das nächste Zeichen als Sonderzeichen, Literal oder oktales Escapezeichen. So stimmt zum Beispiel „n" mit dem Zeichen „n" überein; \n stimmt mit dem Zeichen für eine neue Zeile überein. Die Abfolge \\ stimmt mit \ überein, und \(stimmt mit (überein.
^	Stimmt mit der Position am Anfang der Eingabezeichenfolge überein.
$	Stimmt mit der Position am Ende der Eingabezeichenfolge überein.
*****	Stimmt mit Null oder mehr Vorkommen des vorstehenden Unterausdrucks überein. Beispielsweise stimmt zo* mit z und zoo überein. * ist äquivalent mit {0,}.
+	Stimmt mit einer oder mehr Vorkommen des vorstehenden Unterausdrucks überein. Beispielsweise stimmt zo+ mit zo und zoo überein, aber nicht mit z. + ist äquivalent mit {1,}.
?	Stimmt mit Null oder einem Vorkommen des vorstehenden Unterausdrucks überein. Beispielsweise stimmt do(es)? stimmt mit der Teilzeichenfolge do in do und in does überein. ? ist äquivalent mit {0,1}.
{n}	n ist eine nicht negative ganze Zahl. Stimmt mit genau n Vorkommen des vorstehenden Unterausdrucks überein. Beispielsweise stimmt o{2} nicht mit dem o in Bob, aber mit den beiden o in food überein.
{n,}	n ist eine nicht negative ganze Zahl. Stimmt mit mindestens n Vorkommen des vorstehenden Unterausdrucks überein. Beispielsweise stimmt o{2,} nicht mit dem o in Bob, aber mit allen o in foooood überein. o{1,} ist äquivalent mit o+. o{0}, ist äquivalent mit o*.
{n,m}	m und n sind nicht negative ganze Zahlen mit n <= m. Stimmt mit mindestens n und höchstens m Vorkommen des vorstehenden Unterausdrucks überein. Beispielsweise stimmt o{1,3} mit den ersten drei o in fooooood überein. o{0,1} ist äquivalent mit o?. Beachten Sie, dass zwischen dem Komma und den Zahlen keine Leerzeichen vorhanden sein dürfen.
?	Wenn dieses Zeichen einem der anderen Quantifizierer (*, +, ?, {n}, {n,}, {n,m}) unmittelbar folgt, wird das Muster genügsam („non-greedy"). Ein genügsames Muster stimmt mit dem kürzesten möglichen Teil der durchsuchten Zeichenfolge überein. Dagegen stimmt ein gieriges („greedy") Muster (der Standard) mit dem längsten möglichen Teil der durchsuchten Zeichenfolge überein. Beispielsweise stimmt in der Zeichenfolge oooo der Ausdruck o+? mit einem einzelnen o überein, o+ dagegen mit allen o.
.	Stimmt mit jedem Einzelzeichen außer \n überein. Für eine Übereinstimmung mit jedem Zeichen einschließlich \n verwenden Sie ein Muster wie [.\n].

ZEICHEN	DEFINITION
( )	Gruppiert einen oder mehrere reguläre Ausdrücke, um einen logischen regulären Ausdruck einzurichten, der aus Unterausdrücken besteht. Wird verwendet, um die Standardrangfolge bestimmter Operatoren außer Kraft zu setzen. Übereinstimmungen mit den Klammerzeichen ( ) erreichen Sie mit \(oder \).
x|y	Stimmt mit x oder y überein. Beispielsweise stimmt z|food mit z oder food überein. (z|f)ood stimmt mit zood oder food überein.
[xyz]	Eine Menge von Zeichen. Stimmt mit einem beliebigen der eingeschlossenen Zeichen überein. Beispielsweise stimmt [abc] mit dem a in plain überein.
[^xyz]	Eine negative Menge von Zeichen. Stimmt mit einem beliebigen nicht eingeschlossenen Zeichen überein. Beispielsweise stimmt [^abc] mit dem p in plain überein.
[a-z]	Ein Bereich von Zeichen. Stimmt mit einem beliebigen Zeichen im angegebenen Bereich überein. Beispielsweise stimmt [a-z] mit jedem Kleinbuchstaben im Bereich von a bis z überein.
[^a-z]	Ein negativer Bereich von Zeichen. Stimmt mit einem beliebigen Zeichen überein, das sich nicht im angegebenen Bereich befindet. Beispielsweise stimmt [^a-z] mit jedem Buchstaben außerhalb des Bereichs von a bis z überein.
\b	Stimmt mit einer Wortgrenze überein, d.h. mit der Position zwischen einem Wort und einem Leerzeichen. Beispielsweise stimmt er\b mit dem er in never, aber nicht mit dem er in verb überein.
\B	Stimmt mit der Abwesenheit einer Wortgrenze überein. Beispielsweise stimmt er\B mit dem er in verb, aber nicht mit dem er in never überein.
\cx	Stimmt mit dem durch x angegebenen Steuerzeichen überein. \cM entspricht beispielsweise Strg-M oder einem Wagenrücklaufzeichen. Der Wert von x muss sich im Bereich A-Z oder a-z befinden. Andernfalls wird angenommen, dass es sich bei c um das Literalzeichen c handelt.
\d	Stimmt mit einem Ziffernzeichen überein. Äquivalent mit [0-9].
\D	Stimmt mit einem Nicht-Ziffernzeichen überein. Äquivalent mit [^0-9].
\s	Stimmt mit einem beliebigen Zeichen für Leerraum überein, einschließlich Leerzeichen, Tabulatorzeichen, Seitenvorschub usw. Äquivalent mit [\f\n\r\t\v].
\S	Stimmt mit einem beliebigen Zeichen überein, das nicht für Leerraum steht. Äquivalent mit [^ \f\n\r\t\v].
\w	Stimmt mit jedem Wortzeichen einschließlich des Unterstrichs überein. Äquivalent mit [A-Za-z0-9_].
\W	Stimmt mit jedem Nicht-Wortzeichen überein. Äquivalent mit [^A-Za-z0-9_].
\xn	Stimmt mit n überein, wobei n ein hexadezimales Escapezeichen ist. Hexadezimale Escapezeichen müssen genau zwei Ziffern umfassen. Beispielsweise stimmt \x41 mit A überein. Ermöglicht die Verwendung von ASCII-Codes in regulären Ausdrücken.

Beispiele für reguläre Ausdrücke

Die folgende Tabelle zeigt einige Beispiele für reguläre Ausdrücke und Übereinstimmungen.

AUSDRUCK	ÜBEREINSTIMMUNGEN	KEINE ÜBEREINSTIMMUNGEN
st.n	Austin und Boston	Webster
st[io]n	Austin und Boston	Stanton
st[^io]n	Stanton	Boston oder Austin
^boston	Boston	South Boston oder North Boston Harbor
ston$	Boston und Galveston	Stonewall
sea|side	Seattle und Seaside und Oceanside	Seoul oder Sidney
dal(l|h)art	Dalhart	Dallas oder Lockhart
il?e$	Etoile und Wylie	Beeville
il*e$	Etoile und Wylie und Beeville	Bellaire
il+e$	Etoile und Beeville	Wylie
ad{2}	Addison und Caddo	Adkins
(la.*){2,}	Highland Village und Lake Dallas	Laredo

Rangfolge

Nachdem Sie einen regulären Ausdruck erstellt haben, wird er ähnlich wie ein arithmetischer Ausdruck ausgewertet. Er wird von links nach rechts sowie anhand einer Rangfolge ausgewertet.

Die folgende Tabelle zeigt die Rangfolge für die unterschiedlichen Operatoren in regulären Ausdrücken, beginnend beim höchsten Rang:

ZEICHEN	BESCHREIBUNG
****	Escapezeichen
(), []	Klammern und eckige Klammern
***, +, ?, {n}, {n,}, {n,m}**	Quantifikatoren
^, $, \beliebigesMetazeichen	Anker und Sequenzen
|	Änderung

Anhang B: Administrative Vorlage für ActiveRoles

Mit der administrativen Vorlage **ActiveRoles.adm** können Sie Registrierungseinstellungen mit Hilfe von Gruppenrichtlinien steuern. So können Sie das Verhalten und das Aussehen der Quest One ActiveRoles-Konsole konfigurieren (siehe Quest One ActiveRoles Snap-in-Einstellungen).

Diese administrative Vorlage bietet außerdem eine Reihe von Richtlinieneinstellungen, mit denen Sie die Liste der Verwaltungsdienstinstanzen für die automatische Verbindung von Quest One ActiveRoles beschränken können (siehe Verwaltungsdiensteinstellungen für automatische Verbindung weiter unten).

Quest One ActiveRoles Snap-in-Einstellungen

Mit den Quest One ActiveRoles Snap-in Richtlinien-Einstellungen können Sie:

- Einige Teile der Konsolenbenutzeroberfläche ausblenden.
- Standardeinstellungen für einige Elemente der Benutzeroberfläche festlegen.
- Einstellungen angeben, mit denen Erweiterungs-Snap-Ins bei der Quest One ActiveRoles-Konsole registriert werden.

Die administrative Vorlage bietet die folgenden Richtlinieneinstellungen zur Steuerung des Verhaltens und Aussehens der Quest One ActiveRoles-Konsole:

RICHTLINIEN-EINSTELLUNG	ERKLÄRUNG
Exchange-Verwaltung ausblenden	Entfernt alle Benutzeroberflächenelemente (Befehle, Assistenten und Dialogfelder), mit denen Eigenschaften und Einstellungen im Zusammenhang mit Exchange verwaltet werden können. Wenn Sie diese Richtlinie aktivieren, können Benutzer mit der Quest One ActiveRoles-Konsole keine Aufgaben für Exchange ausführen und keine Exchange-Empfängereinstellungen verwalten. Wenn Sie diese Richtlinie deaktivieren oder sie nicht konfigurieren, können Benutzer mit den entsprechenden Berechtigungen mit der Quest One ActiveRoles-Konsole Aufgaben für Exchange ausführen und Exchange-Empfängereinstellungen verwalten.
Standard-Ansichtsmodus festlegen	Gibt den Ansichtsmodus an, in dem die Quest One ActiveRoles-Konsole gestartet wird. Wenn Sie diese Richtlinie aktivieren, können Sie den Ansichtsmodus in einer Liste auswählen. Die Quest One ActiveRoles-Konsole schaltet beim Start in den ausgewählten Ansichtsmodus um. Benutzer können standardmäßig den Ansichtsmodus mittels des Befehls **Modus**im Menü **Ansicht** ändern. Wenn Sie den Ansichtsmodus erzwingen möchten, wählen Sie die Richtlinienoption **Benutzer nicht zur Änderung des Ansichtsmodus berechtigt** aus. Mit dieser Option wird sichergestellt, dass der Snap-in-Benutzer den von Ihnen ausgewählten Modus verwendet.
Konfigurationsknoten ausblenden	Entfernt den Knoten **Configuration** aus der Konsolenstruktur, wenn sich die Quest One ActiveRoles-Konsole im erweiterten Ansichtsmodus befindet. Wenn Sie diese Richtlinie aktivieren, werden im erweiterten Ansichtsmodus alle Objekte und Container, die im Zusammenhang mit der Quest One ActiveRoles-Konfiguration stehen, nicht angezeigt. Der Knoten **Verwaltete Einheiten** und sein Inhalt sowie alle erweiterten Objekte und Container von Active Directory werden angezeigt.

RICHTLINIEN-EINSTELLUNG	ERKLÄRUNG
Option „Kennwort merken" deaktivieren	Deaktiviert das Kontrollkästchen **Kennwort speichern** im Dialogfeld **Verbindung zum Verwaltungsdienst herstellen**. Wenn Sie diese Richtlinie aktivieren, muss der Benutzer bei jeder Verwendung der Option **Verbinden als: Die Option Folgender Benutzer** auf der Quest One ActiveRoles-Konsole erfordert die Eingabe des Kennworts bei jeder Verwendung der Option. Es kann nicht nach einmaligem Eingeben verschlüsselt und gespeichert werden. Beachten Sie, dass das Speichern von Kennwörtern ein potenzielles Sicherheitsrisiko darstellen kann.
„Verbinden als"-Optionen deaktivieren	Deaktiviert die Optionen **Verbindung als** im Dialogfeld **Verbindung zum Verwaltungsdienst herstellen** einschließlich des Kontrollkästchens **Kennwort speichern**. Wenn Sie diese Richtlinie aktivieren, können die Konsolenbenutzer nur unter ihren Anmeldekonten eine Verbindung zum Verwaltungsdienst herstellen. Bei Verwendung dieser Richtlinie ist die Option **Aktueller Benutzer** unter **Verbinden als** ausgewählt und kann nicht geändert werden.
Standardmäßige Markierung von kontrollierten Objekten aktivieren	Gibt an, ob ein spezielles Symbol zur visuellen Darstellung des Objekts, auf das die Zugriffsvorlagen oder Richtlinienobjekte angewendet (verknüpft) werden sollen, verwendet wird. Wenn Sie diese Richtlinie aktivieren, können Sie Kategorien des Objekts auswählen, das standardmäßig mit einem besonderen Symbol markiert werden soll. Benutzer können diese Einstellung mit dem Befehl **Kontrollierte Objekte markieren** im Menü **Ansicht** ändern.

Außerdem stellt die administrative Vorlage Richtlinien bereit, mit denen Sie Erweiterungs-Snap-Ins bei der Quest One ActiveRoles-Konsole registrieren können. Diese Richtlinien befindet sich im Ordner **Erweiterungs-Snap-ins**. Mit jeder Richtlinie in diesem Ordner wird eines der folgenden Elemente registriert:

RICHTLINIEN-EINSTELLUNG	ERKLÄRUNG
Namespace-Erweiterungen	Registriert Erweiterungs-Snap-Ins, mit denen der Namespace der Quest One ActiveRoles-Konsole erweitert wird.
Kontextmenü-Erweiterungen	Registriert Erweiterungs-Snap-Ins, mit denen ein Kontextmenü auf der Quest One ActiveRoles-Konsole erweitert wird.
Symbolleistenerweiterungen	Registriert Erweiterungs-Snap-Ins, mit denen die Werkzeugleiste der Quest One ActiveRoles-Konsole erweitert wird.
Eigenschaftsblatterweiterungen	Registriert Erweiterungs-Snap-Ins, mit denen Eigenschaftenblätter auf der Quest One ActiveRoles-Konsole erweitert werden.
Aufgabenlistenerweiterungen	Registriert Erweiterungs-Snap-Ins, mit denen eine Aufgabenliste auf der Quest One ActiveRoles-Konsole erweitert wird.
Erweiterungen anzeigen	Registriert Erweiterungs-Snap-Ins, mit denen einer vorhandenen Ansicht Benutzeroberflächenelemente hinzugefügt werden oder mit denen auf der Quest One ActiveRoles-Konsole neue Ansichten erstellt werden.

Wenn Sie eine Richtlinie aus dem Ordner **Erweiterungs-Snap-ins** konfigurieren, werden Sie aufgefordert, den Namen und den Wert des hinzuzufügenden Elements anzugeben.

Der Namensparameter bestimmt den Typ des zu erweiternden Knotens. Jeder Typ wird mit Hilfe einer GUID identifiziert. Wenn Sie beispielsweise Benutzerobjekte erweitern möchten, lautet die GUID {D842D417-3A24-48e8-A97B-9A0C7B02FB17}. Informationen zu anderen Knotentypen finden Sie auf der Quest One ActiveRoles-SDK.

Der Wertparameter bestimmt das hinzuzufügende Erweiterungs-Snap-In. Jedes Snap-In wird mit Hilfe einer GUID identifiziert. Sie können mehrere Snap-Ins hinzufügen, indem Sie ihre GUIDs durch Semikolons getrennt eingeben. Beispielsweise ist folgender Wert möglich:

```
{AD0269D8-27B9-4892-B027-9B01C8A011A1}"Description";{71B71FD3-0C9B-473a-B77B-12FD456FFFCB}"Description"
```

Der Eintrag „`Description`" ist optional und kann beliebigen Text enthalten, der das Erweiterungs-Snap-In beschreibt. Er muss in Anführungszeichen eingeschlossen sein.

Verwaltungsdiensteinstellungen für automatische Verbindung

Die administrative Vorlage bietet die folgenden Einstellungen, mit der Sie die Liste der der Quest One ActiveRoles-Verwaltungsdienstinstanzen für die automatische Verbindung beschränken können:

- Einstellung „Zur automatischen Verbindung zugelassene Server"
- Einstellung „Nicht zur automatischen Verbindung zugelassene Server"
- Einstellung „Server zur automatischen Verbindung"

Auf einem Computer, auf dem eine Quest One ActiveRoles-Client-Anwendung wie die Quest One ActiveRoles-Konsole, Web-Interface oder ADSI Provider läuft, kann die automatische Verbindung der Client-Anwendung mit diesen Einstellungen auf eine vordefinierte Gruppe von Computern mit dem Verwaltungsdienst beschränkt werden. Dabei können bestimmte Computer aus dem Pool der Verwaltungsdienstinstanzen aus der automatischen Verbindung ausgeschlossen oder darin eingebunden werden.

Sie können alle Einstellungen oder nur ausgewählte Einstellungen aktivieren. Wenn die Client-Anwendung sich ausschließlich mit bestimmten Instanzen des Verwaltungsdienstes verbinden soll, können Sie nur die Einstellung **Zur automatischen Verbindung zugelassene Server** aktivieren und konfigurieren. Wenn verhindert werden soll, dass die Client-Anwendung sich automatisch mit bestimmten Instanzen des Verwaltungsdienstes verbindet, können Sie lediglich die Einstellung **Nicht zur automatischen Verbindung zugelassene Server** aktivieren und konfigurieren. Wenn die Client-Anwendung sich automatisch mit einem durch eine Alias identifizierten Server verbindet, aktivieren Sie die Einstellung **Server zur automatischen Verbindung**und fügen Sie den Alias zu dieser Einstellung hinzu.

Die folgenden Regeln gelten, wenn zwei oder mehr Einstellungen aktiviert sind. Wenn der Name eines vorhandenen Rechner sowohl in der Einstellung **Zur automatischen Verbindung zugelassene Server** als auch in **Nicht zur automatischen Verbindung zugelassene Server** erscheint, kann sich die Client-Anwendung automatisch mit den Verwaltungsdienst auf diesem Rechner verbinden. Wenn der Name oder Alias eines bestimmten Rechner in der Einstellung **Server zur automatischen Verbindung** erscheint, verbindet sich die Client-Anwendung automatisch ohne Berücksichtigung der Einstellungen **Zur automatischen Verbindung zugelassene Server** und **Nicht zur automatischen Verbindung zugelassene Server** mit dem Verwaltungsdienst auf diesem Rechner.

Einstellung „Zur automatischen Verbindung zugelassene Server"

Auf einem Computer, auf dem eine Quest One ActiveRoles-Client-Anwendung wie die Quest One ActiveRoles-Konsole, Web-Interface oder ADSI Provider läuft, bestimmt diese Einstellung die Instanzen des Quest One ActiveRoles-Verwaltungsdienstes, mit der die Client-Anwendung automatisch eine Verbindung herstellen kann. Diese Einstellung wirkt sich auf die Verwaltungsdienstinstanzen aus, die von Quest One ActiveRoles zur AutoErmittlung freigegeben wurden. Damit sich die Client-Anwendung mit dem Verwaltungsdienst auf einem Computer verbindet, dessen Name oder Alias nicht zur AutoErmittlung des Verwaltungsdienstes freigegeben wurde, muss die Einstellung **Server zur automatischen Verbindung** verwendet werden.

Wenn Sie diese Einstellung aktivieren, können Sie eine Liste der Computernamen angeben, welche die Computer mit dem Verwaltungsdienst identifiziert, mit denen sich die Client-Anwendung automatisch verbinden darf. In Computernamen kann eine beliebige Zeichenfolge durch einen Platzhalter in Form eines Sternchens (*) ersetzt werden. Wenn ein vorhandener Computer in dieser Einstellung erscheint, darf die Client-Anwendung sich automatisch mit dem Verwaltungsdienst auf diesem Computer verbinden. Wenn ein vorhandener Computer nicht in dieser Einstellung erscheint, darf die Client-Anwendung sich nicht automatisch mit dem Verwaltungsdienst auf diesem Computer verbinden. Das Gegenteil ist nur der Fall, wenn der Name des Computers in der Einstellung **Server zur automatischen Verbindung** erscheint.

Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, verbindet sich die Client-Anwendung normalerweise mit einem beliebigen verfügbaren Verwaltungsdienst, der von Quest One ActiveRoles zur AutoErmittlung freigegeben wurde. Sie können jedoch mit der Einstellung **Nicht zur automatischen Verbindung zugelassene Server** verhindern, dass die Client-Anwendung sich automatisch mit bestimmten veröffentlichten Instanzen des Verwaltungsdienstes verbindet.

Einstellung „Nicht zur automatischen Verbindung zugelassene Server"

Auf einem Computer, auf dem eine Quest One ActiveRoles-Client-Anwendung wie die Quest One ActiveRoles-Konsole, Web-Interface oder ADSI Provider läuft, bestimmt diese Einstellung die Instanzen des Quest One ActiveRoles-Verwaltungsdienstes, mit der die Client-Anwendung nicht automatisch eine Verbindung herstellen kann. Diese Einstellung wirkt sich auf die Verwaltungsdienstinstanzen aus, die von Quest One ActiveRoles zur AutoErmittlung freigegeben wurden.

Wenn Sie diese Einstellung aktivieren, können Sie eine Liste der Computernamen angeben, welche die Computer mit dem Verwaltungsdienst identifiziert, mit denen sich die Client-Anwendung nicht automatisch verbinden darf. In Computernamen kann eine beliebige Zeichenfolge durch einen Platzhalter in Form eines Sternchens (*) ersetzt werden. Wenn ein vorhandener Computer in dieser Einstellung erscheint, darf die Client-Anwendung sich nicht automatisch mit dem Verwaltungsdienst auf diesem Computer verbinden. Das Gegenteil ist nur der Fall, wenn der Name des Computers in der Einstellung **Zur automatischen Verbindung zugelassene Server** oder **Server zur automatischen Verbindung** erscheint.

Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, verbindet sich die Client-Anwendung normalerweise mit einem beliebigen verfügbaren Verwaltungsdienst, der von Quest One ActiveRoles zur AutoErmittlung freigegeben wurde. Mit den Einstellungen **Zur automatischen Verbindung zugelassene Server** und **Server zur automatischen Verbindung** können explizit Instanzen des Verwaltungsdienstes spezifiziert werden, mit denen sich die Client-Anwendung automatisch verbinden sollte.

Einstellung „Server zur automatischen Verbindung"

Auf einem Computer, auf dem eine Quest One ActiveRoles-Client-Anwendung wie die Quest One ActiveRoles-Konsole, Web-Interface oder ADSI Provider läuft, bestimmt diese Einstellung die Instanzen des Quest One ActiveRoles-Verwaltungsdienstes, mit der die Client-Anwendung automatisch eine Verbindung herstellen kann, unabhängig davon, ob diese Instanzen von Quest One ActiveRoles zur AutoErmittlung freigegeben wurden.

Wenn Sie diese Einstellung aktivieren, können Sie eine Liste mit Computernamen oder Aliasen erstellen, welche die Computer mit Verwaltungsdienst identifiziert, mit denen sich die Client-Anwendung automatisch verbindet, obwohl sie den Verwaltungsdienst auf diesen Computern nicht mittels des Dienst-Verbindungspunkts von Quest One ActiveRoles im Active Directory ermitteln kann. Wenn ein bestimmter Computer in dieser Einstellung erscheint, verbindet sich die Client-Anwendung automatisch mit dem Verwaltungsdienst auf diesem Computer, unabhängig von den Einstellungen **Zur automatischen Verbindung zugelassene Server** und **Nicht zur automatischen Verbindung zugelassene Server**.

Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, verbindet sich die Client-Anwendung normalerweise mit einem beliebigen verfügbaren Verwaltungsdienst, der von Quest One ActiveRoles zur AutoErmittlung freigegeben wurde. Mit den Einstellungen **Zur automatischen Verbindung zugelassene Server** und **Nicht zur automatischen Verbindung zugelassene Server** können die automatischen Verbindungen der Client-Anwendung explizit auf zur AutoErmittlung freigegebene Verwaltungsdienste beschränkt werden.

Installationsanweisungen

Gehen Sie wie folgt vor, um mit dem Gruppenrichtlinien-Editor die administrative Vorlage hinzuzufügen oder zu entfernen:

1. Öffnen Sie das Gruppenrichtlinienobjekt, in dem Sie die administrative Vorlage hinzuzufügen oder entfernen möchten.
2. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste unter dem Zweig **Benutzerkonfiguration** oder **Computerkonfiguration** auf **Administrative Vorlagen** und dann auf **Vorlagen hinzufügen/entfernen**.
3. Führen Sie einen der nachfolgend aufgeführten Schritte aus:
   - Um die Vorlage hinzuzufügen, klicken Sie auf **Hinzufügen**. Suchen Sie im Dialogfeld **Richtlinienvorlagen** die Vorlagendatei **ActiveRoles.adm**, wählen Sie sie aus und klicken Sie dann auf **Öffnen**.
   - Um die Vorlage zu entfernen, klicken Sie in der Liste **Aktuelle Richtlinienvorlagen** auf die Vorlage **ActiveRoles** und klicken Sie dann auf **Entfernen**.

Nachdem Sie die Datei ActiveRoles.adm zum Gruppenrichtlinienobjekt hinzugefügt haben, können Sie die Richtlinieneinstellungen konfigurieren, indem Sie in der Konsolenstruktur **Quest One ActiveRoles Snap-in Einstellungen** unter **Benutzerkonfiguration/Administrative Vorlagen** oder **Verwaltungsdienst Einstellungen automatische Verbindung** unter **Computerkonfiguration/ Administrative Vorlagen** auswählen und dann das gewünschte Gruppenrichtlinienobjekt anwenden.

Anhang C: Ports für Datenübertragung

In diesem Abschnitt finden Sie eine Liste der Ports für Datenübertragung, die in der Firewall geöffnet sein müssen, damit Quest One ActiveRoles ordnungsgemäß funktioniert.

Zugriff auf die verwaltete Umgebung

Wenn die von Quest One ActiveRoles verwaltete Umgebung hinter einer Firewall liegt, müssen die folgenden Ports zwischen dem Verwaltungsdienst von ActiveRoles und der verwalteten Umgebung geöffnet sein.

Zugriff auf DNS-Server

- Port **53** TCP/UDP Inbound/Outbound

Zugriff auf Domänenecontroller

- Port **88** (Kerberos) TCP/UDP Inbound/Outbound
- Port **135** (RPC Endpunktzuordnung) TCP Inbound/Outbound
- Port **139** (SMB/CIFS) TCP Inbound/Outbound
- Port **445** (SMB/CIFS) TCP Inbound/Outbound
- Port **389** (LDAP) TCP/UDP, ausgehend
- Port **3268** (Global Catalog LDAP) TCP, ausgehend
- Port **636** (LDAP SSL) TCP, ausgehend

  Dieser Port ist erforderlich, wenn ActiveRoles für den Domänenzugriff mithilfe von SSL konfiguriert ist.

- Port **3269** (Global Catalog LDAP SSL) TCP, ausgehend

  Dieser Port ist erforderlich, wenn ActiveRoles für den Domänenzugriff mithilfe von SSL konfiguriert ist.

- Der von der RPC-Endpunktzuweisung definierte TCP-Port zur Kommunikation mit dem Domänen-Controller

  Sie können Active Directory-Domänen-Controller so konfigurieren, dass diese bestimmte Port-Nummern für die RPC-Kommunikation verwenden. Anweisungen finden Sie unter http://support.microsoft.com/kb/224196.

Zugriff auf Exchange-Server

- Port **135** (RPC Endpunktzuordnung) TCP Inbound/Outbound
- Der von der RPC-Endpunktzuweisung definierte TCP-Port zur Kommunikation mit dem Exchange-Server

  Sie können Exchange-Server so konfigurieren, dass diese bestimmte Port-Nummern für die RPC-Kommunikation verwenden. Anweisungen finden Sie unter http://support.microsoft.com/kb/224196.

Computer-Ressourcenverwaltung

- Port **139** (SMB/CIFS auf den verwalteten Computern) TCP eingehend/ausgehend
- Port **445** (SMB/CIFS auf den verwalteten Computern) TCP eingehend/ausgehend

Computerneustart

- Port **139** (SMB/CIFS auf den verwalteten Computern) TCP eingehend/ausgehend
- Port **137** (WINS) UDP ausgehend
- Port **138** (NetBIOS-Datagramme) UDP ausgehend

Bereitstellung/Auflösung des Startordners

- Port **139** (SMB/CIFS auf den Servern mit den Startordnern) TCP eingehend/ausgehend
- Port **445** (SMB/CIFS auf den Servern mit den Startordnern) TCP eingehend/ausgehend

Zugriff auf SMTP-Server zur E-Mail-Integration

- Port **25** (SMTP-Standard-Port) TCP ausgehend

  ActiveRoles verwendet standardmäßig SMTP-Port 25. Die standardmäßige Port-Nummer kann in den Eigenschaften des Mail-Konfigurationsobjekts in der ActiveRoles-Konsole geändert werden. Definiert die Mail-Konfiguration einen anderen Port, öffnen Sie diesen an Stelle von Port 25.

Zugriff auf AD LDS-Instanzen

- Der bei der Registrierung der AD LDS-Instanz mit Quest One ActiveRoles angegebene TCP-Port

Zugriff auf SQL Server

Befindet sich der SQL Server mit der ActiveRoles-Datenbank hinter der Firewall, müssen Sie die folgenden Ports zwischen ActiveRoles Administration Service und SQL Server öffnen:

- Port **1433** (SQL Server-Standardinstanz) TCP eingehend/ausgehend

  Öffnen Sie diesen Port, wenn sich Ihre ActiveRoles-Datenbank auf der SQL Server-Standardinstanz befindet. Wird der Standardinstanz ein anderer Port zugewiesen, öffnen Sie diesen an Stelle von Port 1433.

- Port **1434** (SQL Server Browser-Dienst) UDP eingehend/ausgehend

  Öffnen Sie diesen Port, wenn sich Ihre ActiveRoles-Datenbank auf einer benannten SQL Server-Standardinstanz befindet. In diesem Fall verwendet ActiveRoles UDP-Port 1434, um den Port zu ermitteln, der der benannten Instanz zugewiesen wurde. Daher müssen Sie Port 1434 zusammen mit dem TCP-Port öffnen, der der benannten Instanz zugewiesen wurde.

Zugriff auf ActiveRoles Administration Service

Wenn Sie eine Firewall zwischen ActiveRoles-Clients UND ActiveRoles Administration Service platzieren möchten (z. B. MMC Interface, Web Interface, ADSI Provider oder Management Shell), müssen Sie die folgenden Ports in der Firewall öffnen:

- Port **135** (RPC Endpunktzuordnung) TCP Inbound/Outbound
- Der von der RPC-Endpunktzuweisung definierte TCP-Port zur Kommunikation mit Administration Service

ActiveRoles verwendet Distributed COM (DCOM) über zwei separate TCP-Ports zur Annahme von Client-Verbindungen und Anforderungen. Port 135 wird von ActiveRoles-Clients zur Lokalisierung von Administration Service verwendet. Anschließend werden alle Anfragen von ActiveRoles-Clients über den Port gesendet, der dynamisch von der RPC-Endpunktzuweisung definiert wird. Anweisungen zur Konfiguration der dynamischen RPC-Port-Zuweisung finden Sie unter support.microsoft.com/kb/154596.

Zugriff auf Web Interface

Wenn Sie über eine Firewall auf ActiveRoles Web Interface zugreifen möchten, müssen Sie die folgenden Ports öffnen:

- Port **80** (Standard-HTTP) TCP eingehend/ausgehend
- Port **443** (Standard-HTTPS) TCP eingehend/ausgehend

Web Interface wird normalerweise über Port 80 ausgeführt, bzw. über Port 443, wenn SSL aktiv ist (standardmäßig inaktiv).